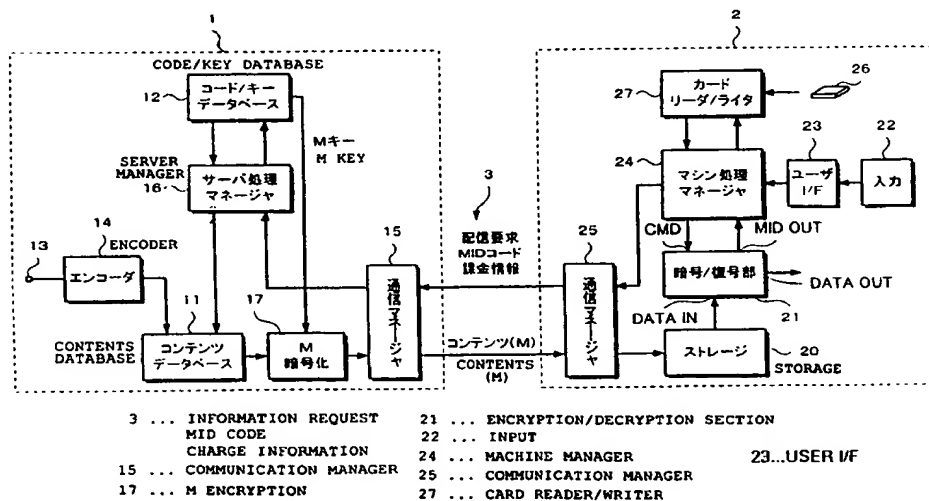


(51) 国際特許分類6 G06F 17/60, 17/30, 15/00	A1	(11) 国際公開番号 WO99/59092 (43) 国際公開日 1999年11月18日(18.11.99)
(21) 国際出願番号 PCT/JP99/02404 (22) 国際出願日 1999年5月10日(10.05.99) (30) 優先権データ 特願平10/127227 1998年5月11日(11.05.98) JP (71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP) (72) 発明者; および (75) 発明者/出願人 (米国についてのみ) 勝又 泰(KATSUMATA, Yasushi)[JP/JP] 大林正之(OHBAYASHI, Masayuki)[JP/JP] 中津山孝(NAKATSUYAMA, Takashi)[JP/JP] 韓 敏哉(KAN, Toshiya)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP) (74) 代理人 弁理士 杉浦正知(SUGIURA, Masatomo) 〒170-0013 東京都豊島区東池袋1丁目48番10号 25山京ビル420号 Tokyo, (JP)	(81) 指定国 CN, IN, KR, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE) 添付公開書類 国際調査報告書	

(54)Title: APPARATUS FOR DATA DISTRIBUTION, AND TERMINAL FOR DATA DISTRIBUTION

(54)発明の名称 データ配信装置及びデータ配信用の端末装置



(57) Abstract

A contents server comprises a contents database that stores the data of contents encrypted with a C key and the C key. The data of contents encrypted with the C key, together with the C key, are encrypted with an M key, and sent to a user machine. In the user machine, the data of contents encrypted with the C key and the C key are stored in a storage device. For reproduction, the data of contents encrypted with the C key and the C key are sent from the storage device to an encryption/decryption section and decrypted. The user is charged on the basis of the C key. A DA code, which changes dynamically with time, is appended to the C key.

コンテンツサーバには、Cキーにより暗号化されたコンテンツのデータと、Cキーとが蓄積されるコンテンツデータベースを設ける。Cキーにより暗号化されたコンテンツのデータと、Cキーを、Mキーで暗号化して、ユーザマシンに送る。ユーザマシンでは、Cキーにより暗号化されたコンテンツのデータと、Cキーをストレージデバイスに保存する。再生時にストレージデバイスからのCキーにより暗号化されたコンテンツのデータと、Cキーを、暗号化／復号化処理部に送り、復号すると共に、Cキーに応じて課金を行なう。また、Cキーに、時間と共に動的に変化するDAコードを付加する。

PCTに基づいて公開される国際出願のパフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AL	アルバニア	EE	エストニア	LC	セントルシア	SD	スーダン
AM	アルメニア	ES	スペイン	LI	リヒテンシュタイン	SE	スウェーデン
AT	オーストリア	FI	フィンランド	LK	スリランカ	SG	シンガポール
AU	オーストラリア	FR	フランス	LR	リベリア	SI	スロヴェニア
AZ	アゼルバイジャン	GA	ガボン	LS	レソト	SK	スロヴァキア
BA	ボスニア・ヘルツェゴビナ	GB	英国	LT	リトアニア	SL	シエラ・レオネ
BB	バルバドス	GD	グレナダ	LU	ルクセンブルグ	SN	セネガル
BE	ベルギー	GE	グルジア	LV	ラトヴィア	SZ	スワジランド
BF	ブルキナ・ファソ	GH	ガーナ	MA	モロッコ	TD	チャード
BG	ブルガリア	GM	ガンビア	MC	モナコ	TG	トーゴ
BJ	ベナン	GN	ギニア	MD	モルドヴァ	TJ	タジキスタン
BR	ブラジル	GW	ギニア・ビサウ	MG	マダガスカル	TZ	タンザニア
BY	ベラルーシ	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア 共和国	TM	トルクメニスタン
CA	カナダ	HR	クロアチア	ML	マリ	TR	トルコ
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	TT	トリニダード・トバゴ
CG	コンゴ	ID	インドネシア	MR	モリタニア	UA	ウクライナ
CH	スイス	IE	アイルランド	MW	マラウイ	UG	ウガンダ
CI	コートジボアール	IL	イスラエル	MX	メキシコ	US	米国
CM	カメルーン	IN	インド	NE	ニジェール	UZ	ウズベキスタン
CN	中国	IS	アイスランド	NL	オランダ	VN	ヴェトナム
CR	コスタ・リカ	IT	イタリア	NZ	ニュージーランド	YU	ユーゴスラビア
CU	キューバ	JP	日本	NO	ノルウェー	ZA	南アフリカ共和国
CY	キプロス	KE	ケニア	NZ	ニュージーランド	ZW	ジンバブエ
CZ	チェコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

明 細 書

データ配信装置及びデータ配信用の端末装置

5 技術分野

この発明は、例えば、複数の音楽データが蓄積されるコンテンツサーバと、このコンテンツサーバに蓄積されたコンテンツから所望のコンテンツが配信されるユーザマシンとからなる情報配信システムに関するもので、特に、コンテンツの保護と課金に係わる。

10

背景技術

近年、インターネットや衛星通信の普及により、コンピュータネットワーク網を利用した種々のサービスが実現されつつある。そのようなコンピュータネットワーク網を使ったサービスのひとつとして、以下のよ

15 うな音楽配信サービスを行なうシステムが提案されている。

第14図において、501はコンテンツサーバ、502はユーザマシンである。コンテンツサーバ501には、複数の音楽データがコンテンツとして蓄積されている。ユーザマシン502には、ハードディスクドライブや光ディスクドライブ等のストレージデバイス504が接続され

20 ると共に、課金を行なうためのカードリーダー／ライター505が接続される。カードリーダー／ライター505には、カード506が装着される。

音楽配信サービスを利用する場合には、ユーザマシン502が伝送路503を介してコンテンツサーバ501に接続される。伝送路503は、例えば、インターネットのようなコンピュータネットワーク網である

25 。ユーザマシン502がコンテンツサーバ501に接続されると、コンテンツサーバ501からユーザマシン502にコンテンツのリストや検

索画面が送られる。

ユーザは、このコンテンツのリストや検索画面で所望のコンテンツを検索して、ダウンロードしたいコンテンツを選択する。ユーザがコンテンツを選択すると、ユーザマシン 502 からコンテンツサーバ 501 に
5 そのコンテンツの要求命令が送られる。コンテンツサーバ 501 で、要求命令に応じてコンテンツが取り出され、このコンテンツがコンテンツサーバ 501 からユーザマシン 502 に送られる。そして、このコンテンツがユーザマシン 502 のストレージデバイス 504 に保存される。

このとき、カードリーダー/ライタ 505 により、適切な課金が行なわれ
10 る。

このような音楽配信システムが普及すると、ユーザは、所望の楽曲の音楽データを通信で簡単に入手することができる。また、このようなシステムにおけるサーバには、検索機能が備えられており、このような検索機能を使うと、所望の楽曲を検索して、入手することが簡単にできる
15 。更に、このようなシステムにおけるサーバでは、常に音楽データの更新が行われるため、最新の楽曲をいち早く入手することができる。

ところが、このようにサーバからの音楽データをユーザマシンに配信するようなシステムでは、コンテンツのデータが無断で複製され、著作権者の権利が守られなくなる危険性がある。このため、コンテンツのデータが無断で複製されることがないように、複製防止のための機能を付加
20 する必要があると共に、コンテンツに対して適切な課金が行なわれる必要がある。

また、このようなシステムでは、ダウンロードした音楽データを他の機器で再生させたり、他人譲渡したりするようなことが考えられる。常に、1 台の機器にのみコンテンツのデータが移動されるようにすれば、
25 不正コピーが出回る可能性はない。ところが、他の機器への複製を一切

禁止してしまうと、このようなコンテンツのデータの移動も行なえなくなってしまう。

したがって、この発明の目的は、コンテンツの配信を行なうようなシステムで、コンテンツの保護が十分図れ、正当な課金が行なえるように

5 した情報配信システムを提供することにある。

発明の開示

この発明は、機器固有の第1の識別データと第1の識別データと対応する第2の識別データとが記憶されている第1の記憶部と、

10 第1の記憶部から読み出された第1の識別データとともにデータの配信要求データを送信するとともに送信されてきたデータを受信する第1の送受信部と、

データ送受信部によって受信されたデータを蓄える第1のデータ記憶部と、

15 第1のデータ記憶部から読み出されたデータを第1の記憶部に記憶されている第2の識別データに基づいて復号化処理を施す第1の信号処理部と、

第1の送受信部によって受信されたデータを第1のデータ記憶部に記憶させる動作を行うとともに第1のデータ記憶部から読み出されたデー

20 タの第1の信号処理部による復号化処理動作を制御する第1の制御部と

、
第1の送受信部から送信されてきた第1の識別データと配信要求データを受信するとともにデータの送信を行う第2の送受信部と、

複数のデータが記憶され、配信要求データに対応するデータを出力する第2のデータ記憶部と、

25 送信されてきた第1の識別データに対応する第2の識別データが記憶さ

れている第2の記憶部と、

第2のデータ記憶部から出力されたデータに第2の記憶部から読み出された第2の識別データに基づいて暗号化処理を施す第2の信号処理部と、

- 5 送信されてきた配信要求データと第1の識別データに基づいて第2の記憶部から第2の識別データの読み出し制御を行うとともに配信要求データに基づいて第2のデータ記憶部からデータの読み出し制御を行う第2の制御部とを備え、

- 第2の送受信部を介して送信されてきた第2の識別データに基づいて
- 10 暗号化されたデータを第1の信号処理部によって復号するデータ配信装置である。

- この発明は、機器固有の第1の識別データと第1の識別データと対応する第2の識別データとが記憶されている第1の記憶部と、第1の記憶部から読み出された第1の識別データとともにデータの配信要求データ
- 15 を送信するとともに送信されてきたデータを受信する第1のデータ送受信部と、データ送受信部によって受信されたデータを蓄える第1のデータ記憶部と、第1のデータ記憶部から読み出されたデータを第1の記憶部に記憶されている第2の識別データに基づいて復号化処理を施す第1の信号処理部と、第1の送受信部によって受信されたデータを第1のデータ記憶部に記憶させる動作を行うとともに第1のデータ記憶部から読み出されたデータの第1の信号処理部による復号化処理動作を制御する
- 20 第1の制御部とを有する少なくともひとつの端末機器部と、

- 端末機器部と伝送路を介して接続され、第1の送受信部から送信されてきた第1の識別データと配信要求データを受信するとともにデータの
- 25 送信を行う第2の送受信部と、複数のデータが記憶され、配信要求データに対応するデータを出力する第2のデータ記憶部と、送信されてきた

-----第1の識別データに対応する第2の識別データが記憶されている第2の-----
記憶部と、第2のデータ記憶部から出力されたデータに第2の記憶部か
ら読み出された第2の識別データに基づいて暗号化処理を施す第2の信
号処理部と、送信されてきた配信要求データと第1の識別データに基づ
5 いて第2の記憶部から第2の識別データの読み出し制御を行うとともに
配信要求データに基づいて第2のデータ記憶部からデータの読み出し制
御を行う第2の制御部とを有するサーバ装置部とを備え、

第2の送受信部を介して送信されてきた第2の識別データに基づいて
暗号化されたデータを第1の信号処理部によって復号するデータ配信装
10 置である。

この発明は、装置固有の第1の識別データと第1の識別データと対応
する第2の識別データとが記憶されている記憶部と、

記憶部から読み出された第1の識別データとともにデータの配信要求
データを送信するとともに第2の識別データによって暗号化されて送信
15 されてきたデータを受信するデータ送受信部と、

データ送受信部によって受信された第2の識別データに基づいて暗号
化されたデータを蓄えるデータ記憶部と、

データ記憶部から読み出されたデータを記憶部に記憶されている第2
の識別データに基づいて復号処理を施す信号処理部と、

20 送受信部によって受信されたデータをデータ記憶部に記憶させる動作
を行うとともにデータ記憶部から読み出されたデータの信号処理部によ
る復号化処理動作を制御する制御部とを備えているデータ配信用の端末
装置である。

25 図面の簡単な説明

第1図はこの発明が適用できるデータ配信システムにおけるMキーを

用いたシステムの説明に用いるブロック図である。第2図はこの発明が適用できるデータ配信システムにおけるMキーを用いたシステムの暗号化／復号化処理部の説明に用いるブロック図である。第3図はこの発明が適用できるデータ配信システムにおけるCキーを用いたシステムの説明に用いるブロック図である。第4図はこの発明が適用できるデータ配信システムにおけるCキーを用いたシステムの暗号化／復号化処理部の説明に用いるブロック図である。第5図はこの発明が適用できるデータ配信システムにおけるCキーを用いたシステムの説明に用いるフローチャートである。第6図はこの発明が適用できるデータ配信システムにおけるTキーを用いたシステムの説明に用いるブロック図である。第7図はこの発明が適用できるデータ配信システムにおけるTキーを用いたシステムの暗号化／復号化処理部の説明に用いるブロック図である。第8図A及び第8図Bはこの発明が適用できるデータ配信システムにおけるTキーを用いたシステムにおける暗号化／復号化処理部の説明に用いるブロック図である。第9図はこの発明が適用できるデータ配信システムにおけるDAコードを用いたシステムの説明に用いるブロック図である。第10図はDAコードの説明に用いる略線図である。第11図はこの発明が適用できるデータ配信システムにおけるDAコードを用いてシステムの暗号化／復号化処理部の説明に用いるブロック図である。第12図はこの発明が適用できるデータ配信システムにおけるDAコードを用いたシステムの説明に用いるフローチャートである。第13図はこの発明が適用できるデータ配信システムにおけるDAコードを用いたシステムの説明に用いるフローチャートである。第14図は従来のデータ配信システムの一例のブロック図である。

25

発明を実施するための最良の形態

-----以下、この発明の実施の形態について図面を参照して説明する。-----この

発明は、コンテンツのデータを転送するようなシステムにおいて、コンテンツのデータの保護が図れると共に、適切な課金が行なえるようにしたものである。このようなシステムに用いられる暗号化キーやコード

5 について先ず簡単に説明しておく。

1. キー及びコードの説明

この発明が適用されたシステムでは、以下のような暗号化キーやコードが用いられる。

(1) Mキー

10 M (Machine) キーの役割は、特定の機器、後述するユーザーマシンでのみデータを利用可能とすることである。Mキーは例えば機器の工場出荷時に各機器毎に与えられるもので、各機器固有の暗号化情報である。Mキーは、保護を図るために、例えば機器の暗号化／復号化処理部内に埋め込まれ、機器内から外へは取り出せないようになっている。

15 (2) MIDコード

各機器には、固有のMID (Machine Identification) コードが付与される。このMIDコードも、工場出荷時に各機器に付与される。MIDコードは、各機器を特定するためにのみ使用されるものであり、直接的に暗号化キーとして用いられるものではない。したがって、外部に漏
20 れても、データの保護が守られなくなる危険性は少ない。MIDコードは、Mキーと同様に、例えば機器の暗号化／復号化処理部内に埋め込んでおいても良いし、別のROMやEEPROMに蓄えておいても良い。

(3) Cキー

25 C (Contents) キーの役割は、各コンテンツ毎にデータの保護を図ることである。ここで、コンテンツとは、移動できる1かたまりの情報の

単位とする。すなわち、データを課金するようなシステムでは、1つの課金の対象となる情報の単位である。音楽サーバのような場合には、1曲毎に課金をするとすると、各曲の音楽データという単位が1つのコンテンツのデータとなる。

- 5 各コンテンツは、各コンテンツに固有のCキーを用いて暗号化される。したがって、そのコンテンツに対応するCキーを有しているユーザ側の機器でのみ、そのCキーを使ってコンテンツの暗号を解読して、再生することが可能である。このように、Cキーを有しているユーザ側の機器でのみ、そのコンテンツを利用可能なことから、Cキーは、そのコンテンツ
- 10 コンテンツを利用できる権利を表すキーという見方もできる。

(4) Tキー

- T (Transfer) キーの役割は、各ユーザ機器間でデータの移動を行う際に、データの保護を図るためのものである。各機器間でコンテンツの移動を行うような場合に、Cキーが外部に漏れる可能性がある。このため、各機器間でデータの移動を行う場合には、Cキーと、Cキーで暗号
- 15 化されたコンテンツは、更に、Tキーで暗号化される。

- Tキーは、データの受け取り側の機器と、データの送り側の機器との間で予め決められたアルゴリズムで、M I Dコードに基づいて生成される。すなわち、機器間でコンテンツのデータの移動を行う場合には、受け取り側の機器から送り側の機器に対して、受け取り側のM I Dコード
- 20 が送られる。送り側の機器では、送られてきたM I Dコードに基づいて、Tキーが生成される。また、受け取り側の機器では、自分のM I Dコードに基づいて、同様のアルゴリズムによりTキーが生成される。

(5) D Aコード

- 25 暗号／復号化チップ内で生成される動的認証コードであり、Cキーに付加される。D Aコードは、例えば、乱数、タイムコード等を利用して

生成される。このようなD-Aコードを付加しておくことで、Cキーを一時的に退避させてコンテンツを不正使用することができなくなる。また、D-Aコードを利用して、所定の期間使用を許可／禁止したり、コンテンツを貸し借りしたりすることができるようになる。

5 2. Mキーを使ったシステムについて

第1図は、この発明が適用されたデータ配信システムの一例を示すものである。この例は、Mキーと呼ばれる暗号化キーを導入して、特定の端末機器でのみデータを利用可能にするようにしたものである。

第1図において、コンテンツサーバ1は伝送路3によってユーザマシン2と結ばれている。尚、第1図ではコンテンツサーバ1に伝送路3を介して接続される端末機器としてのユーザマシン2は説明を簡単にするために1個しか描かれていないが、実際にはサーバ1に伝送路3を介して複数のユーザマシン2が接続される。コンテンツサーバ1には、コンテンツデータベース11が設けられる。このコンテンツデータベース11には、コンテンツサーバ1で提供するコンテンツのデータが格納されている。

コンテンツデータベース11に格納されるコンテンツのデータは、コンテンツ入力端子13から入力、供給される。例えば、音楽配信サービスを行なうサーバの場合には、コンテンツ入力端子13から音楽データが供給される。この音楽データは、エンコーダ14に供給される。エンコーダ14で、この音楽データが例えば、特開平3-139923号や特開平3-139922号等を開示されている変形DCT (Modified Discrete Transform) : 所謂ATRA C (Adaptive Transform Acoustic Coding) で圧縮符号化される。この圧縮された音楽データがコンテンツデータベース11に蓄えられる。

コンテンツサーバ1には、RAMやハードディスクドライブから構成

されるコード及びキーデータベース 1 2 が設けられる。このコード及び
キーデータベース 1 2 には、コンテンツサーバ 1 に繋がれる全ての機器
としてのユーザマシン 2 の M I D コードと M キーとが蓄えられる。M I
D コードは、各ユーザマシン 2 を識別するためのユーザマシン毎の固有
5 の情報である。M キーは、各ユーザマシン毎に固有の暗号化キーである。
M I D コード及び M キーは例えば機器の工場出荷時に各ユーザマシン
2 に与えられる。M I D コード及び M キーを工場出荷時に各ユーザマシン
2 に付与する際に、各機器毎に付与した M I D コード及び M キーのリ
ストに基づいてコード及びキーデータベース 1 2 に記憶されるデータが
10 生成される。

コンテンツサーバ 1 の全体動作は、サーバ処理マネージャ 1 6 により
管理されている。コンテンツサーバ 1 の通信制御は、通信マネージャ 1
5 により管理されている。コンテンツサーバ 1 からのデータは、暗号化
回路 1 7 により暗号化される。このときの暗号化は、ユーザマシン 2 か
15 ら送られてきた M I D コードに基づいてコード及びキーデータベース 1
2 で検索された M キーに基づいて行なわれる。

一方、端末機器としてのユーザマシン 2 には、暗号化／復号化処理部
2 1 が設けられる。この暗号化／復号化処理部 2 1 は、データの暗号化
処理及び暗号の復号化処理を行う専用の I C より構成されている。この
20 暗号化／復号化処理部 2 1 には、工場出荷時に、機器固有の M I D コー
ドと、M キーが格納されている。

第 2 図は、暗号化／復号化処理部 2 1 の構成を示すものである。暗号
化／復号化処理部 2 1 には、M キーホルダ 5 1 と、M I D コードホルダ
5 2 と、M キー復号化回路 5 3 と、コントローラ 5 4 が設けられる。M
25 キーホルダ 5 1 には、各機器固有の暗号化情報である M キーが工場出荷
時に記憶される。M I D コードホルダ 5 2 には、各機器固有の識別情報

であるM I Dコードが工場出荷時に記憶される。コントローラ5 4は、暗号化／復号化処理部2 1の動作を制御している。

コントローラ5 4には、後述するマシンマネージャから送信されてくるコマンドがコマンド端子C M Dに供給される。このコマンドに基づいて、暗号化／復号化処理部2 1の動作が設定される。Mキー復号化回路5 3には、入力端子D A T A _ I NからMキーで暗号化されたコンテンツのデータが供給される。Mキー復号化回路5 3には、Mキーホルダ5 1からMキーが供給される。Mキー復号化回路5 3で、入力端子D A T A _ I Nから入力コンテンツのデータの暗号解読を行なわれる。Mキー復号回路5 3の出力データは、データ出力端子D A T A _ O U Tから出力される。M I Dコードホルダ5 2からは、コード出力端子M I D _ O U Tが導出される。このコード出力端子M I D _ O U Tからは、M I Dコードが出力される。

第2図に示すように、暗号化／復号化の処理は、1チップのI Cから構成される暗号化／復号化処理部2 1で行われ、この暗号化／復号化処理部2 1内に、Mキーと、M I Dコードが格納されている。このため、外部からは、暗号化／復号化処理部2 1での暗号処理がどのようにして行われ、暗号化キーが何であるのかは解明できない。

第1図において、ユーザマシン2には、入力部2 2からユーザによって操作された結果としての入力供給される。入力部2 2からの入力は、ユーザインターフェース2 3を介して、マシン処理マネージャ2 4に与えられる。

マシン処理マネージャ2 4は、マイクロコンピュータ等から構成され、ユーザマシン2の全体処理を行っている。マシン処理マネージャ2 4は、入力部2 2からコンテンツサーバ1のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理部2 1にコマンドを与え、M I D

コードを問い合わせる動作を行なう。暗号化／復号化処理部 21 は、M I D コードの問い合わせコマンドが供給されると、供給された M I D の問い合わせコマンドに対応して、M I D コードホルダ 52（第 2 図）に記憶されている M I D コードをマネージャ 24 に出力する。

- 5 マシン処理マネージャ 24 は、暗号化／復号化処理部 21 から M I D コードを受け取ったら、通信マネージャ 25 に、配信要求と、M I D コードと、課金情報を送る。これら配信要求、M I D コード、課金情報は、通信処理マネージャ 25 から、伝送路 3 を介して、ユーザマシン 2 からコンテンツサーバ 1 の通信マネージャ 15 に送られる。

- 10 コンテンツサーバ 1 からのコンテンツのデータの配信サービスを受ける場合には、カード 26 が装着される。このカード 26 の残高情報がカードリーダー／ライター 27 を介してマシン処理マネージャ 24 に送られる。コンテンツの配信が実行されると、マシン処理マネージャ 24 は、カードリーダー／ライター 27 を介して、カード 26 に、引き出し指示、もしくは減額指示を与え、カード 26 から、コンテンツの配信に応じた代金が差し引かれる。このようにして、コンテンツにの配信に対する代金の支払いがコンテンツ配信を行っている会社に対して行なわれる。このとき、正規のユーザか否か、ユーザが確かに課金を行っているか否かをチェックしてから、ユーザマシン 22 から送信されてきた M I D コードに
- 15 対応する M キーを出力させるようにしても良い。

- コンテンツサーバ 1 側では、マイクロコンピュータなどから構成されるサーバ処理マネージャ 16 がサーバ 1 の全体処理の制御を行なっている。通信マネージャ 15 がユーザマシン 2 から送信されてくる配信要求、M I D コード、課金情報を受信すると、受信した配信要求、M I D コード、課金情報は、サーバ処理マネージャ 16 に送られる。
- 25

 サーバ処理マネージャ 16 は、ユーザマシン 2 から送信されてきた M I D

コードを受信したら、このM-I-Dコードをコード及びキーデータベース
12に送り、ユーザマシン2から送信されてきたM I Dコードに対応す
るユーザマシンのMキーを問い合わせるコマンドをベース12に供給す
る。コード及びキーデータベース12は、前述したようにサーバ1に接
5 続される各機器毎のM I Dコードと、M I Dコードに対応するMキーの
情報が予め格納されており、コード及びキーデータベース12は、マネ
ージャ16から送信されてきたM I Dコードを受け付けると、送信され
てきたM I Dコードからユーザマシン2を識別し、M I Dコードを送信
してきたユーザマシン2に対応するMキーを出力する。送信されてきた
10 M I Dコードに対応するMキーは、Mキー暗号化回路17に送られる。
ベース12から送信されてきたMキーに基づいてMキー暗号化回路17
に、暗号化キーがセットされる。

サーバ処理マネージャ16は、ユーザマシン2からの配信要求を受け
付けると、要求されたコンテンツの配信指示を示すコマンドをコンテ
15 ツデータベース11に送る。コンテンツデータベース11は、ユーザマ
シン2の配信指示を受け取ると、送信されてきた配信指示に対応するコ
ンテンツのデータの読み出しを行なう。データベース11から読み出さ
れたコンテンツのデータは、Mキー暗号化回路17に送られる。

Mキー暗号化回路17には、コード及びキーデータベース12から、
20 データを要求したユーザマシン2の機器のM I Dコードに対応したMキ
ーがセットされている。コンテンツデータベース11から送られるコン
テンツのデータは、Mキー暗号化回路17で、上述したユーザマシン2
のM I Dコードに対応するMキーにより暗号化される。Mキーで暗号化
されたコンテンツのデータは、コンテンツサーバ1の通信マネージャ1
25 5から、伝送路3を介して、ユーザマシン2の通信路マネージャ25に
送られる。このコンテンツのデータは、ユーザマシン2にあるストレー

ジデバイス 20 に蓄積される。ここで、伝送路 3 としては、ISDN (Integrated Servises Digital Network) 等の有線又は無線の通信網を伝送路として用いることができる。

- このように、ユーザマシン 2 からコンテンツサーバ 1 にコンテンツの
- 5 配信を要求する際に、ユーザマシン 2 からコンテンツサーバ 1 に、ユーザマシン 2 の機器固有の MID コードが送られる。コンテンツサーバ 1 には、コード及びキーデータベース 12 が設けられており、このコード及びキーデータベース 12 から、ユーザマシン 2 から送られてきたユーザマシン 2 の MID コードに対応する M キーが呼び出され、データベース
- 10 ス 11 から読み出されたコンテンツのデータがこの M キーで暗号化される。ユーザマシン 2 の機器固有の M キーで暗号化されたコンテンツのデータがユーザマシン 2 に送られ、暗号化されたコンテンツのデータがユーザマシン 2 のストレージデバイス 20 に蓄えられる。ストレージデバイス 20 に蓄えられたコンテンツのデータは、ユーザマシン 2 の機器固有の M キーで暗号化されているので、コンテンツの配信を要求したユーザマシン 2 以外では配信されてきたコンテンツのデータの復号が行なえない。これにより、サーバ 1 からユーザマシン 2 に配信されるコンテンツの著作権を守ることができる。

- すなわち、ストレージデバイス 20 に蓄えられたコンテンツのデータ
- 20 を復号する場合には、ストレージデバイス 20 から、読み出されたコンテンツのデータは第 2 図における暗号化／復号化処理部 21 のデータ入力端子 DATA__IN に供給される。第 2 図に示したように、暗号化／復号化処理部 21 の M キーホルダ 51 には、ユーザマシン 2 の機器固有の M キーが蓄えられている。コンテンツサーバ 1 から送られてきたコンテンツのデータは、MID コードホルダ 52 の MID コードに対応する
- 25 M キーで暗号化されているため、コンテンツサーバ 1 側の M キー暗号化

回路1-7に設定されたMキーは、ユーザマシン2のMキーホルダ5-1に格納されているMキーと同様である。したがって、ストレージ20から読み出されたMキーで暗号化されたコンテンツのデータは、暗号化／復号化処理部21で、復号することができる。

- 5 これに対して、ストレージデバイス20に蓄えられていたコンテンツのデータを、ユーザマシン2以外のユーザマシン又は機器に複製したとする。ストレージデバイス20に蓄えられていたコンテンツのデータは、ユーザマシン2の機器固有のMキーで暗号化されている。他の機器の暗号化／復号化処理部21は、複製元となるユーザマシン2の機器と同じのMキーを有していない。このため、ストレージデバイス20に蓄えられていたコンテンツのデータを本来のユーザマシン2、即ちサーバ1に配信要求を送ってサーバ1から送信されてきたコンテンツのデータを蓄えていたユーザマシン2以外の機器に複製したとしても、複製元となる機器では、コンテンツのデータの暗号を解読できない。

15 3. Cキーを使ったシステムについて

- 第1図及び第2図に示すMキーを導入することで、特定の機器でのみコンテンツのデータが利用可能となる。ところが、Mキーだけでは、サーバ1から配信されてきたコンテンツのデータを記憶したユーザマシンからコンテンツのデータを他のユーザマシンや機器に移動させることが一切できなくなってしまう。コンテンツのデータが限りなく複製されてしまうと著作権者の権利が守られなくなることが考えられるが、コンテンツのデータが移動されただけなら、コンテンツのデータを利用する機器が移っただけなので、問題は生じない。上述した第1図、第2図に示すように、Mキーだけを用いる装置、方法では、上述したようなコンテンツのデータの或る機器から他の機器、すなわち、或るユーザマシンから他のユーザマシンへの移動に対応できない。ユーザマシンに一度蓄積し

ておいたコンテンツのデータがエラーになってしまったり、ダウンロードに失敗したりするようなことが考えられる。このような場合、正規のユーザが正当な課金をしてそのコンテンツのデータの配信を受けているなら、再度、そのコンテンツのデータを配信し直すことが望まれる。コンテンツには有料のコンテンツと無料のコンテンツがあり、Mキーのみでは、コンテンツの種類に応じて適切な課金が行なえない。

上述したように、Mキーを導入することで、各機器としての各ユーザマシンを単位とするコンテンツのデータの保護、不正なコンテンツデータの複製に対する保護は図れるが、Mキーだけでは、各コンテンツ毎のデータの保護を図り、適切な課金を行なうには不十分である。そこで、コンテンツ毎の暗号化を行うCキーを導入した例を第3図以下を用いて説明する。

第3図には、Cキーを導入したデータ配信システムの一例が示されている。Cキーの役割は、各コンテンツ毎にデータの保護を図ることである。

Cキーを導入したデータ配信システムにおいては、ユーザマシン102側の暗号化／復号化処理部121として、第2図に示した暗号化／復号化処理部21と同様に、第4図に示すように、Mキーホルダ151と、MIDコードホルダ152と、Mキー復号化回路153と、コントローラ154とが設けられると共に、更に、処理部121には、Cキー取り込み回路155と、Cキー復号化回路156とが設けられる。Mキーホルダ151、MIDコードホルダ152、Mキー復号化回路153、コントローラ154の動作は、前述のMキーのみのデータ配信システムにおける暗号化／復号化処理部21と同様であり、Mキーホルダ151には、各ユーザマシン102の機器固有の暗号化情報であるMキーが工場出荷時に記憶され、MIDコードホルダ152には、各ユーザマシン

-----1-0-2の機器固有の識別情報であるM-I-Dコードが工場出荷時に記憶され、コントローラ 1 5 4 は、暗号化／復号化処理部 1 2 1 の動作を制御している。Cキー取り込み回路 1 5 5 は、Mキーの解読により復号されたCキーを保持するものである。Cキー復号回路 1 5 6 は、Cキーによる復号化処理を行なうものである。

コントローラ 1 5 4 には、後述するマシン処理マネージャからコマンド端子CMDからコマンドが供給され、このコマンド端子CMDから供給されてくるコマンドに基づいて、暗号化／復号化処理部 1 2 1 の動作が設定される。Mキー復号化回路 1 5 3 には、入力端子DATA_IN
10 から、Cキーで暗号化され更にMキーで暗号化されたデータと、入力端子KEY_INからのMキーで暗号化されたCキーが供給される。Mキー復号化回路 1 5 3 には、Mキーホルダ 5 1 から、Mキーが供給される。

入力データの暗号化キー、すなわち、DATA_INから供給される
15 データを暗号化しているMキーがMキーホルダ 1 5 1 からのMキーと一致していれば、Mキー復号化回路 1 5 3 で、暗号解読を行なえる。Mキー復号化回路 1 5 3 からは、Mキーによる暗号化の解かれたCキーと、Cキーで暗号化されたデータが出力される。このCキーがCキー取り込み回路 1 5 5 に保持され、Cキーで暗号化されたデータがCキー復号化
20 回路 1 5 6 に供給される。

Cキー復号化回路 1 5 6 で、Cキーに基づく復号化処理が行なわれ、Cキーで暗号化されているデータが解読される。このCキー復号回路 1 5 6 の出力データは、データ出力端子DATA_OUTから出力される。
MIDコードホルダ 1 5 2 からは、コード出力端子MID_OUTが
25 導出される。このコード出力端子MID_OUTからは、MIDコードが出力される。暗号化／復号化処理部 1 2 1 には、Cキーで暗号化され

てデータを転送するために、Cキーの出力端子KEY__OUTと、Cキーで暗号化されたコンテンツのデータの出力端子DATA__Tが設けられる。

このように、Cキーを導入したデータ配信システムにおいては、第3
5 図におけるユーザマシン102側の暗号化／復号化処理部121として、第4図に示すような構成のものが用いられる。第3図に示すように、コンテンツサーバ101側には、Cキーを発生するCキー生成部118と、Cキー生成部118によって生成されたCキーを使って、コンテンツのデータを暗号化するCキー暗号化回路119が設けられる。それ以
10 外の構成については、前述の第1図に示したコンテンツサーバ1と同様に構成されている。

前述のMキーだけのデータ配信システムでは、コンテンツ入力端子13からのデータは、エンコーダ14で圧縮符号化されて、そのままコンテンツデータベース11に蓄積されたが、第3図に示す例では、コンテ
15 ンツ入力端子113からのデータは、エンコーダ114で圧縮符号化された後、Cキー暗号化回路119に送られ、Cキー生成部118からのCキーによりCキー暗号化回路118で暗号化されて、コンテンツデータベース111に蓄積される。このときの暗号化回路119で用いられたCキーがコンテンツデータベース111に蓄積される。

20 ユーザがコンテンツサーバ101のコンテンツの配信を受けたい場合には、ユーザがユーザマシン102の入力部122を操作してユーザインターフェース123を介して、マシン処理マネージャ124にコンテンツ配信を指示する入力を与えられる。

マシン処理マネージャ124は、入力部122からコンテンツサーバ
25 101のコンテンツを獲得すべき入力を受け付けると、暗号化／復号化処理部121にコマンドを与え、MIDコードを問い合わせる。暗号化

／復号化処理部 1 2 1 は、マシン処理マネージャ 1 2 4 から送信されてきたコマンドが与えられると、このコマンドに対応して、M I D コードを出力する。

マシン処理マネージャ 1 2 4 は、暗号化／復号化処理部 1 2 1 から M I D コードを受け取ったら、通信マネージャ 1 2 5 に、配信要求と、M I D コードと、課金情報を送る。配信要求、M I D コード及び課金情報の各情報は、通信処理マネージャ 1 2 5 から、伝送路 1 0 3 を介して、コンテンツサーバ 1 0 1 の通信マネージャ 1 1 5 に送られる。

通信マネージャ 1 1 5 は、ユーザマシン 1 0 2 からの M I D コードが供給されると、供給された M I D コードをサーバマネージャ 1 1 6 に送る。サーバマネージャ 1 1 6 は、コード及びキーデータベース 1 1 2 にユーザマシン 1 0 2 から送信されてきた M I D コードを送り、送信してきた M I D コードに対応する M キーを問い合わせるコマンドを送信する。コード及びキーデータベース 1 1 2 は、ユーザマシン 1 0 2 から送信されてきた M I D コードに対応する機器の M キーを出力する。コード及びキーデータベース 1 1 2 から出力される M キーは、M キー暗号化回路 1 1 7 に供給され、M キー暗号化回路 1 1 7 にユーザマシン 1 0 2 から送信されてきた M I D コードに対応する M キーがセットされる。

サーバ処理マネージャ 1 1 6 は、ユーザマシン 1 0 2 からの配信要求を受け付けると、要求されたコンテンツの配信指示のコマンドをコンテンツデータベース 1 1 1 に送る。コンテンツデータベース 1 1 1 は、サーバ処理マネージャ 1 1 6 からの情報に基づいて、ユーザマシン 1 0 2 の配信要求と対応するコンテンツのデータを読み出す。

前述したように、コンテンツデータベース 1 1 1 のデータは、C キーにより暗号化されている。したがって、C キーにより暗号化されたコンテンツデータが、更に、M キー暗号化回路 1 1 7 により、M キーで暗号

化される。また、このときのCキーがコンテンツデータベース111から読み出され、Mキー暗号化回路117により、Mキーにより暗号化される。

このように、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーは、コンテンツサーバ101の通信マネージャ115から、伝送路103を介して、ユーザマシン102の通信路マネージャ125に送られる。伝送路103を介してサーバ101より送信されてきたCキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーは、ユーザマシン102のストレージデバイス120に蓄積される。

このように、コンテンツデータベース111に蓄えられているコンテンツのデータはCキーで暗号化されており、コンテンツサーバ101からユーザマシン102にデータが送られる際に、更に、Cキーで暗号化されたデータは、Mキーで暗号化されている。Cキーで暗号化されたコンテンツのデータを解読するためには、Cキーが必要であるが、このCキーは、コンテンツサーバ1から、Mキーで暗号化されてユーザマシン102に供給されている。

ストレージデバイス120に蓄えられたコンテンツのデータを復号する場合には、ストレージデバイス120から読み出されたコンテンツのデータは、第4図における暗号化／復号化処理部121のデータ入力端子DATA_INに供給される。Mキーで暗号化されたCキーが、ストレージデバイス120から読み出されて、暗号化／復号化処理部121のキー入力端子KEY_INに供給される。

第4図に示すように、暗号化／復号化処理部121のMキーホルダ151には、ユーザマシン102の機器固有のMキーが蓄えられている。コンテンツサーバ101から送られてきたコンテンツのデータは、MI

Dコードホルダ152のM-I-Dコードに対応するMキーで暗号化されている。コンテンツサーバ101側のMキー暗号化回路117に設定されたMキーは、Mキーホルダ151に格納されているMキーと同じである。したがって、ストレージデバイス120からの、Cキーで暗号化され
5 更にMキーで暗号化されたコンテンツのデータは、Mキーに基づく暗号化部分は、Mキー復号化回路153で、復号することができる。

同様に、ストレージデバイス120からのMキーで暗号化されたCキーは、Mキー復号化回路153で復号される。

したがって、Mキー復号化回路153からは、Cキーで暗号化された
10 データと、Cキーが出力される。このCキーは、Cキー取り込み回路155に供給され、Cキーで暗号化されたデータは、Cキー復号回路156に供給される。Cキー復号回路156で、Cキーによる暗号の解読が行われ、コンテンツのデータが復号される。この復号されたデータがデータ出力端子DATA_OUTから出力される。Cキー取り込み回路
15 155から出力されるCキーがキー出力端子KEY_OUTから出力される。

このようにコンテンツのデータをCキーで暗号化しておくと、コンテンツのデータを利用するときには、必ず、これを解読するためのCキーが必要になる。Cキーを有しているユーザ側のユーザマシン又は機器で
20 のみ、コンテンツのデータを利用することができるので、Cキーは、そのコンテンツのデータを利用できる権利を表すキーとして用いることができる。

すなわち、1つの端末機器としての或るユーザマシンから他の端末機器としての他のユーザマシンにCキーを送れば、コンテンツのデータと
25 そのコンテンツのデータを利用する権利が送られたことになり、他のユーザ側の端末機器で、そのコンテンツのデータを利用することができる

。このように1つの端末機器から他のユーザ側の端末機器にCキーを送った後にその機器のCキーを消去してしまうと、たとえ送り側の機器にコンテンツのデータが残っていても、そのコンテンツのデータに付加されているCキーによる暗号を解くことができないので、コンテンツデータは、最早利用できない。換言すると、そのコンテンツデータを他のユーザ側の機器に若しくは他のユーザに譲渡したという見方ができる。

正規のユーザが誤ってコンテンツのデータを消してしまったり、コンテンツのデータのダウンロードに失敗してしまうような場合がある。この場合でも、ユーザマシン102にCキーが残っていれば、そのコンテンツのデータをサーバ101より再送してもらい、残っているCキーを用いて再送してもらったコンテンツのデータを解読し、コンテンツのデータを利用することができる。このように、Cキーを導入することにより、以下のように、コンテンツのデータの移動や再送が行なえるようになる。Cキーを利用することにより、課金の設定を行なうことができる。

暗号化／復号化処理部121のキー出力端子KEY__OUTからのCキーと、データの出力端子DATA__TからのCキーで暗号化されたデータを移動先となる相手側の機器としてのユーザマシンに転送し、データの転送が終わったら、Cキー取り込み回路155に保存されているCキー及びストレージデバイス120に保存されているCキーを消去することで、コンテンツのデータの移動が行なわれる。このようにすると、相手側の機器でのみコンテンツのデータの利用が可能となる。このとき、移動元ともるユーザマシンのストレージデバイス120に残っているコンテンツのデータは、消去しなくても良い。なぜなら、移動元となるユーザマシンのストレージデバイス120に残っているコンテンツのデータは、Cキーで暗号化されており、Cキーが消去されてしまえば、そ

-----のコンテンツのデータは解読することができないので、コンテンツのデータとして利用できないからである。

この場合とは逆に、ストレージデバイス 120 のコンテンツのデータを消去してしまった後でも、C キーが保存されていれば、コンテンツのデータをサーバ 101 より再送してもらえれば再びコンテンツのデータの
5 利用ができる。コンテンツのデータの再送は、前述のコンテンツのデータのダウンロードの場合と同様の処理で行なわれる。このとき、新規のコンテンツのデータの配信、すなわち、ダウンロードであるか否かを C キーで判断し、新規の場合のみ、課金を行なうようにする。例えば、
10 ユーザマシン 102 が送信されてきた C キーをコンテンツ / C キーデータベース 111 で照合することによって、いつの時点で C キー生成部 118 で生成された C キーであるかによって新規のコンテンツのデータの配信であるか否かを判別する。

上述したように、C キーを使うと、コンテンツのデータの配信の内容
15 に応じた課金が行なえる。例えば、無料のコンテンツのデータに対しては C キーを付加せず、有料のコンテンツのデータにのみ C キーを付加するようにしても良い。受信側、すなわちユーザマシン 102 側では、サーバ 101 より送られてきた C キーが新規のものであるか否かをマシン処理マネージャ 124 が判断し、新規の C キーの場合のみ、課金を行な
20 うようにする。このようにすると、サーバ 101 から送信されてくる C キーに基づいてサーバ 101 から引き出そうとしているコンテンツ又はコンテンツのデータが有料のコンテンツ又はコンテンツのデータであるか否かを判断することができ、有料のコンテンツ又はコンテンツのデータの保護が図れる。上述のコンテンツのデータの再送のような場合には
25 、ユーザマシン 102 に保存されている C キーと、受信されたコンテンツのデータを暗号化している C キーとを比較し、この比較結果から、上

述したように、課金を行なうかどうかを判断することができる。更に、課金に関する情報（例えば、コンテンツのランク付け等）をコード化してCキーに包含させておき、同じコンテンツに対して条件により料金を変更できるようにすることも可能である。

- 5 第5図は、Cキーを使った課金処理を示すフローチャートである。サーバ101から配信されてきたデータをユーザマシン102のストレージデバイス120に取り込む際に、すなわち、ダウンロードの際に、ユーザマシン102の暗号化／復号化部121のキー出力端子KEY__OUTより出力されたか否か、すなわち、Cキーが受信されたか否かが判断される（ステップS1）。Cキーが受信されなければ、サーバ101から配信されてきたコンテンツのデータが無料のコンテンツのデータであるとして、課金を行なわれない（ステップS2）。Cキーが受信されたら、ストレージデバイス120にCキーが保存されているか否かが判断される（ステップS3）。コンテンツの再送のような場合には、ストレージデバイス120にCキーが保存されているので、受信されたCキーと、ストレージデバイス120に保存されているCキーとが一致するか否かを判断する（ステップS4）。受信されたCキーと、ストレージデバイス120に保存、記憶されているCキーとが一致している場合には、コンテンツのデータの再送であるので、課金を行なわれない（ステップS2）。

- ステップS3でサーバ101から送信されてきたCキーがストレージデバイス120にCキーが保存されていないと判断された場合、又はステップS4で、受信されたCキーとストレージデバイス120に保存されているCキーとが一致していないと判断された場合には、Cキーの課金ランクの情報が取得される（ステップS5）。この課金ランクの情報に応じて、課金処理が行なわれる（ステップS6）。Cキーの課金ラン

ク情報とは、例えばコンテンツのデータの種類やデータの品質を表す情報等が考えられる。

4. Tキーを使ったシステムについて

上述したように、Cキーをデータ配信システムに導入することで、コンテンツのデータの或る機器としてのユーザマシンと他の機器としてのユーザマシンとの間の移動、コンテンツデータの再送が行なえるようになる。ところが、Cキーのみでは、移動先となる相手側の機器にコンテンツの移動を行なう際に、Cキーが直接送信される。このとき、Cキーが外部に漏れて、コンテンツのデータの保護が図られなくなる可能性がある。データ移動時のコンテンツのデータの保護を図るために、Tキーをデータ配信システムに導入した例を以下に説明する。

第6図は、Tキーを導入したデータ配信システムの一例を示すものである。第6図において、データの送り側のユーザマシン202Aは、上述した第3図に示したデータ配信システムのユーザマシン102と同様に、ストレージデバイス220A、暗号化／復号化処理部221A、入力部222A、ユーザインターフェース223A、マシン処理マネージャ224A、通信マネージャ225A、カードリーダー／ライタ227Aから構成される。カードリーダー／ライタ227Aには、上述した第3図に示したデータ配信システムで用いられるカード126と同様のカード226Aが装着される。

データの受信側のユーザマシン202Bは、上述したユーザマシン202Aと同様に前述した第3図に示したデータ配信システムのユーザマシン102のように、ストレージデバイス220B、暗号化／復号化処理部221B、入力部222B、ユーザインターフェース223B、マシン処理マネージャ224B、通信マネージャ225B、カードリーダー／ライタ227Bから構成される。カードリーダー／ライタ227Bには

、上述したカード 2 2 6 A と同様のカード 2 2 6 B が装着される。

T キーを導入したデータ転送システムでは、暗号化／復号化処理部 2 2 1 A 及び 2 2 1 B として、第 7 図に示すようなものが用いられる。第 7 図に示すように、暗号化／復号化処理部 2 2 1 A 及び 2 2 1 B には、
5 M キーホルダ 2 5 1 と、M I D コードホルダ 2 5 2 と、M キー復号化回路 2 5 3 と、コントローラ 2 5 4 と、C キー取り込み回路 2 5 5 と、C キー復号化回路 2 5 6 とが設けられると共に、T キー暗号化回路 2 5 7 と、T キー生成回路 2 5 8、2 5 9 と、T キー復号化回路 2 6 0 と、M キー暗号化回路 2 6 1 とが設けられる。

10 M キーホルダ 2 5 1、M I D コードホルダ 2 5 2、M キー復号化回路 2 5 3、コントローラ 2 5 4 の動作は、前述までのデータ配信システムにおけるユーザマシン 2、1 0 2 の暗号化／復号化処理部 2 1、1 2 1 と同様であり、M キーホルダ 2 5 1 には、各ユーザマシンの機器固有の暗号化情報である M キーが工場出荷時に記憶され、M I D コードホルダ
15 2 5 2 には、各機器固有の識別情報である M I D コードが工場出荷時に記憶されている。コントローラ 2 5 4 は、暗号化／復号化処理部 2 2 1 A、2 2 1 B の動作を制御する。C キー取り込み回路 2 5 5 は、M キーの解読により復号された C キーを保持し、C キー復号回路 2 5 6 は、C キーの復号化処理を行なう。

20 T キー暗号化回路 2 5 7 は、T キー生成回路 2 5 8 からの T キーにより、他の機器としての他のユーザマシン 2 0 2 B に或る機器としての或るユーザマシン 2 0 2 A から移動するデータを T キーで暗号化するものである。T キー復号回路 2 6 0 は、T キー生成回路 2 5 9 からの T キーにより、移動されてきたデータを復号するものである。T キー生成回路
25 2 5 8 及び 2 5 9 は、M I D コードに基づいて T キーを生成するものである。

第8図A及び第8図Bは、ユーザマシン202Aからユーザマシン202Bに、コンテンツのデータを移動するときの暗号化／復号化処理部221A、221Bの動作を説明するためのものである。

ユーザマシン202Aからユーザマシン202Bにコンテンツのデータ
5 タを移動する際には、データを送出する側のユーザマシン202Aから、相手側のユーザマシン202BにMIDコードの転送要求が送られる。

相手側のユーザマシン202Bでは、MIDコードの送信要求を受け付けると、ユーザマシン202Bの暗号化／復号化処理部221BのMIDホルダ252BからMIDコードを呼び出し、MIDホルダ252Bから読み出されたMIDコードがコード出力端子MID__OUTから出力され、このMIDコードは、ユーザマシン202Bから、ユーザマシン202Aに送信される。

データを送出する側のユーザマシン202Aでは、コード入力端子MID__INから相手側のユーザマシン202Bから送信されてきたMIDコードを受信すると、受信したMIDコードをTキー生成回路258Aに供給する。Tキー生成回路258Aは、この相手側のユーザマシン202Bから送られてきたMIDコードに基づいて、Tキーを生成する。Tキー生成回路258Aで生成されたTキーがTキー暗号化回路257Aに供給される。

ユーザマシン201Aは、ユーザマシン202BからのMIDコードを受信し、Tキー暗号化回路257Aに受信したMIDコードに基づいてTキーが生成され、Tキー暗号化回路257Aに供給されたら、ユーザマシン201Aからユーザマシン201Bへのコンテンツのデータ及びCキーの送信をするための動作が開始される。

ユーザマシン202Aのストレージデバイス220Aには、Cキーで

暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーが蓄積されている。したがって、ユーザマシン202Aからユーザマシン202Bにコンテンツのデータ及びCキーを送信する際に、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータと、Mキーで暗号化されたCキーが、ユーザマシン202Aのストレージデバイス220Aから、暗号化／復号化処理部221Aのキー入力端子KEY__IN及びデータ入力端子DATA__INに供給される。

Mキー復号化回路253Aには、Mキーホルダ251AからMキーが供給される。Mキー復号化回路253Aで、Mキーホルダ251AからのMキーによりMキーに基づいて施されている暗号の復号処理が行なわれる。このMキー復号回路253Aからは、復号化されたCキーとCキーで暗号化されたコンテンツのデータが出力される。復号回路253Aから出力されるCキーは、Cキー取り込み回路255Aに供給されると共に、Tキー暗号化回路257Aに供給される。復号回路253Aから出力されるCキーで暗号化されたコンテンツのデータは、Cキー復号化回路256Aに供給されると共に、Tキー暗号化回路257Aに供給される。

Cキー復号化回路256Aで、復号回路253Aから供給されるCキーで暗号化されたコンテンツのデータの復号化処理が行なわれ、コンテンツのデータに施されているCキーに基づく暗号の復号化処理が行なわれる。復号されたコンテンツのデータは、データ出力端子DATA__OUTから出力される。

Tキー暗号化回路257Aには、Tキー生成回路258Aでユーザマシン202BのMIDコードに基づいて生成されたTキーが設定されている。Mキー復号回路253Aから出力されるCキー及びCキーで暗号

化されたコンテンツのデータは、Tキー暗号化回路257Aで、相手側のユーザマシン202BのMIDコードに基づいて生成されたTキーで暗号化される。したがって、Tキー暗号化回路257Aからは、Tキーで暗号化されたCキーと、Cキーで暗号化され更にTキーで暗号化されたコンテンツのデータが出力される。

このTキーで暗号化されたCキーと、Cキーで暗号化され更にTキーで暗号化されたコンテンツのデータは、キー出力端子TKEY_OUT及びデータ出力端子TDATA_OUTから出力され、相手側のユーザマシン202Bに送られ、相手側のユーザマシン202Bの暗号化／復号化処理部221Bのキー入力端子RCKEY_IN及びデータ入力端子RDATA_INに入力され、Tキー復号化回路260Bに供給される。ユーザマシン202BにTキーで暗号化されたCキーとCキー及びTキーで暗号化されたコンテンツのデータの送信が完了した時点で、ユーザマシン202Aのストレージデバイス220Aに記憶されているCキーは削除され、ストレージデバイスからのコンテンツのデータの読み出しが禁止される。

Tキー復号化回路260Bには、Tキー生成回路259Bから、Tキーが与えられる。このTキーは、Tキー生成回路259BでMIDホルダ252BからのMIDコードに基づいて生成されている。

送り側のユーザマシン202Aでは、ユーザマシン202Bから送信されてくるMIDコードを受信し、Tキー生成回路258Aで、受信したMIDコードに基づいて、Tキーを生成している。受信側のユーザマシン202BのTキー復号化回路260Bでは、MIDコードホルダ252BからのMIDコードに基づいてTキーを生成している。Tキー生成回路258AとTキー生成回路259Bには、同一のMIDコードが送られている。したがって、ユーザマシン202Aから送られてきたT

キーによって各々暗号化されているコンテンツのデータ及びCキーは、ユーザマシン202BのTキー復号回路260Bで復号化することができる。

5 Tキー復号化回路260Bからは、Cキーと、Cキーで暗号化されたコンテンツのデータが出力される。このCキーと、Cキーで暗号化されたコンテンツのデータは、Mキー暗号化回路261Bに供給される。

Mキー暗号化回路261Bには、Mキーホルダ251Bから、ユーザマテン202Bの機器固有のMキーが与えられる。Mキーホルダ251
10 Bから読み出されたMキーに基づいて、Cキーと、Cキーで暗号化されたコンテンツのデータが暗号化される。したがって、Mキー暗号化回路261Bからは、Mキーで暗号化されたCキーと、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータが出力される。Mキー暗号化回路261Bから出力されるMキーで暗号化されたCキーと、Cキーで暗号化され更にMキーで暗号化されたコンテンツのデータは、キー
15 出力端子RKEY_OUT及びデータ出力端子RDATA_OUTから各々出力され、ユーザマシン202Bのストレージデバイス220Bに記憶保存される。

このように、Tキーを用いると、ユーサマシン202Aからユーザマシン202Bにデータを移動する際に、ユーサマシン202Aからユー
20 ザマシン202Bに送信されるCキー及びCキーで暗号化されたコンテンツのデータは、更にTキーで暗号化される。このため、外部に暗号化キーとしてのCキーが漏れることがなく、コンテンツのデータの保護が図れる。

5. DAコードを用いたシステム

25 上述したように、Tキーをデータ配信システムに導入すると、或る機器としてのユーザマシンと他の機器としてのユーザマシンとの間にデー

タを移動させる際のデータ保護を図ることができる。しかしながら、上
述したように、Tキーを導入したとしても、同一の機器内でデータを移
動することは可能である。例えば、Cキーを同一のユーザマシン内の別
の場所、例えば別な記憶部に一時的に保存しておいてから、コンテンツ
5 のデータの移動を行ない、その後、Cキーを元に戻すようなことを行
なうと、コンテンツデータの移動によってCキーは消去されてしまうが
、Cキーが別な場所に別途保存されているので、保存されているCキー
を用いれば、コンテンツのデータが不正に複製されてしまう。

そこで、Cキーに、時間と共に動的に変化するコード（DAコードと
10 称する）を付加して、Cキーに時間的に変化する要素を持たせることが
考えられる。以下、時間的に変化する要素を有するCキーを用いたデー
タ配信システムについて第9図以下に説明する。

つまり、第9図において、ユーザマシン302は、Cキー保存メモリ
330以外は前述した第3図に示したユーザマシン102と同様に、ス
15 トレージデバイス320、暗号化／復号化処理部321、入力部322
、ユーザインターフェース323、マシン処理マネージャ324、通信
マネージャ325、カードリーダー／ライター327から構成される。カー
ドリーダー／ライター327には、前述した第3図に示したカード126と
同様のカード326が装着される。

20 このようなユーザマシン302で、例えばストレージデバイス320
からCキーを読み出し、ストレージデバイス320から読み出されたこ
のCキーをCキー保存メモリ330に保存しておいてから、ストレージ
デバイス320のコンテンツのデータを他の機器としての他のユーザマ
シンに移動したとする。この場合、コンテンツのデータの移動が終了す
25 ると、ストレージデバイス320のCキーは消されるが、Cキー保存メ
モリ330にCキーを退避させているので、メモリ330のCキーは消

去されない。その後、Cキー保存メモリ 330からのCキーをストレージデバイス 320に戻せば、ストレージデバイス 320にコンテンツのデータが残っていれば、他のユーザマシンに移動したはずのコンテンツのデータを復号できてしまう。更に、ストレージデバイス 320にコンテンツデータが無くても、Cキーがあれば、前述したようにコンテンツサーバ1からコンテンツのデータの再送が要求を行なうことができ、コンテンツデータの不正使用が可能となる。

そこで、本データ配信システムでは、第10図に示すように、Cキーに、時間と共に動的に変化するDAコードが付加される。このDAコードとしては、タイムコードや乱数が用いられる。このように、CキーにDAコードを付加することにより、上述したようなコンテンツのデータの不正利用を防止することができる。

第11図は、第10図に示したDAコードが付加されたCキーを扱うための暗号化／復号化処理部 321の構成を示すものである。暗号化／復号化処理部 321には、第7図に示した暗号化／復号化処理部 221A、221Bと同様に、Mキーホルダ 351と、MIDホルダ 352と、Mキー復号化回路 353と、コントローラ 354と、Cキー取り込み回路 355と、Cキー復号化回路 356と、Tキー暗号化回路 357と、Tキー生成回路 358、359と、Tキー復号化回路 360と、Mキー暗号化回路 361とが設けられると共に、DAコード管理回路 362とが設けられる。

DAコード管理回路 362は、Cキーに付加するDAコードの管理を行なうものである。すなわち、DAコード管理回路 362は、所定時間毎にストレージデバイス 320からのCキーを呼び出しを行なう。Cキーが呼び出されると、CキーのDAコードのチェックを行い、DAコードが正しければ、DAコードの更新処理を行なう。

なお、ストレージデバイス320には、Mキーで暗号化されたCキーが保存されている。したがって、このMキーで暗号化されたCキーは、
先ず、キー入力端子KEY_INから、Mキー復号化回路353に送られて、Mキーに基づいて施されている暗号化の復号処理が行なわれる。

- 5 Mキー復号化回路353から、復号されたCキーが出力され、このCキーは、DAコード管理回路362に送られる。

- DAコード管理回路362は、復号化回路353から供給されるCキーのDAコードを所定時間毎に検出して正しく更新されているDAコードがCキーに付加されているか否かを判断し、Cキーに付加されている
10 正しく更新されているDAコードなら、DAコードの更新を行なう。このDAコードが更新されたCキーをMキー暗号化回路361に供給して再びMキーに基づいて暗号化処理を行なって、再び、ストレージデバイス320に保存する。Cキーに付加されているDAコードのタイムコードである場合にはタイムコードが所定の規則に従って変化しているもの
15 であるか否かを判断することによって行なわれるようにしても良く、後述するステップS13で用いている手法に基づいて判断しても良い。

- 第12図は、DAコード管理回路362の処理を示すフローチャートである。第12図において、例えばコントローラ354又はDAコード管理回路362のタイマ機能によって所定時間経過したか否かが判断され（ステップS11）、所定時間経過したら、ストレージデバイス320よりCキーが読み出されて復号化回路353で復号され、復号されたCキーに付加されているDAコードが検出される（ステップS12）。
ストレージデバイス320より読み出されたDAコードが正しく更新されているDAコードであるか否かが判断される（ステップS13）。こ
25 のステップS13でDAコードが正しく更新されているか否かは、暗号化／復号化処理部31内に保持しているDAコードとストレージデバイ

ス 3 2 0 から読み出された D A コードが一致しているか否かにより判断できる。ステップ S 1 3 で正しく更新されている D A コードであると判断されると、この D A コードが次の D A コードに更新され、そして、この更新された D A コードが付加された C キーは、再び、M キー暗号化回路 3 6 1 によって M キーに基づいて暗号化処理が施されてストレージデバイス 3 2 0 に戻される（ステップ S 1 4）。

ステップ S 1 3 で、検出された D A コードが正しく更新されている D A コードではないと判断されたら、ストレージデバイス 3 2 0 の C キーを消去し、又は、C キーに不正利用を示すコードを付加して、D A コードが正しく更新されていないと判断された C キーに対応するそのコンテンツのデータの利用が禁止される（ステップ S 1 5）。

このように、ストレージデバイス 3 2 0 の C キーが正常に扱われている場合には、D A コード管理回路 3 6 2 で、C キーに付加される D A コードが所定の時間毎に絶えず更新され、更新された D A コードが付加された C キーがストレージデバイス 3 2 0 に保存される。

例えば、C キーを第 9 図における C キー保存メモリ 3 3 0 に保存しておいたような場合には、C キー保存メモリ 3 3 0 に保存されている C キーの D A コードが上述のように更新されないので、D A コード管理回路 3 6 2 で、D A コードが正しくないと判断される。その結果、前述したように C キーを一旦メモリ 3 3 0 に保存しておいてコンテンツのデータの移動を行ない、移動後にメモリ 3 3 0 に保存されている C コードを用いてコンテンツのデータの不正利用を行なうことを防止できる。

上述したように、動的に変化する D A コードを使うと、ある期間再生を禁止／許可することができるようになる。これを利用すると、コンテンツを所定の期間貸し出したり、コンテンツの利用に試用期間を設定したりすることができる。

第13図は、上述したような動的に変化するD Aコードを有するCキーを用いて所定期間だけコンテンツのデータを再生可能に設定する場合の処理を示すフローチャートである。なお、第13図に示す場合、D Aコードとしては、タイムコードが用いられる。このCキーのD Aコードには、更に、期限情報が付加される。

第13図において、上述したステップS11と同様にして所定時間経過したか否かが判断され（ステップS21）、所定時間経過したら、ストレージデバイス320に保存されているCキーが呼び出される。上述したステップS12と同様に、このCキーに付加されているD Aコードが検出される（ステップS22）。D Aコードが正しく更新されているか否かが判断される（ステップS23）。ステップS23で正しく更新されているD Aコードであると判断されると、このD Aコードが次のD AコードにD Aコード管理回路362で更新される（ステップS24）。この更新されたD Aコードに付加されている期限情報とコンテンツデータの使用期限を示し、D Aコード管理コードに保持されている期限情報とが比較され、Cキーが使用期限超過か否かが判断される（ステップS25）。Cキーが使用期限超過でなければ、この更新されたD Aコードが付加されたCキーがストレージデバイス320に戻され（ステップS26）、ステップS21リターンされる。

ステップS23で、ストレージデバイス320から呼び出されたD Aコードが正しく更新されているものではないと判断されたら、ストレージデバイス320からCキーが削除され、又は、Cキーに不正使用を示すコードが付加されて、D Aコードが正しく更新されていないと判断されたCキーに対応するコンテンツのデータの利用不可能とされる。（ステップS26）。ステップS25で、Cキーの使用期間超過であると判断されると、ステップS26に移行し、ストレージデバイス320から

Cキーが削除され、又は、Cキーに不正使用を示すコードが付加されて、上述と同様に使用期限超過と判断されたCキーに対応するコンテンツのデータの利用不可能とされる。

このようにして、DAコードを用いて、ある期間だけコンテンツのデータの再生を禁止又は許可したりすることができる。これにより、試用期間を設けて、ユーザがコンテンツのデータを再生させるようなことができる。更に、一方のユーザマシンから他方のユーザマシンにコンテンツのデータを移動する場合に、一方のユーザマシンのCキーをDAコードにより所定の期限まで再生禁止とし、他方のユーザマシンのCキーをその期間のみ再生可能とすると、一方のマシンから他方のマシンに所定の期間だけコンテンツのデータを貸すような制御が行なえる。

この発明によれば、コンテンツサーバに保存されるコンテンツは、Cキーで暗号化されている。このように、Cキーを設けることにより、コンテンツを移動したり、再送を要求したりできる。また、送られてきたCキーと同一のCキーがストレージデバイスに保存しているか否かを判断することにより、再送か否かを判断して、適切な課金を行ったり、Cキーにランクを付けてコンテンツ毎に料金を変えて課金を行なうようなことができる。

また、この発明によれば、Cキーに、時間と共に動的に変化するDAコードが付加される。このようなDAコードを付加することで、Cキーを退避させておいて、コンテンツを不正利用するようなことが防止できる。また、この時間と共に動的に変化するDAコードを利用して、コンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借するようなことが行なえる。

25

産業上の利用可能性

-----以上のように、この発明にかかるデータ配信装置及びデータ配信用の-----
端末装置は、例えば、複数の音楽データが蓄積されるコンテンツサーバ
と、このコンテンツサーバに蓄積されたコンテンツから所望のコンテン
ツが配信されるユーザマシンとからなる情報配信システムに用いて好適
5 である。

請 求 の 範 囲

1. 機器固有の第1の識別データと上記第1の識別データと対応する第2の識別データとが記憶されている第1の記憶部と、

- 5 上記第1の記憶部から読み出された上記第1の識別データとともにデータの配信要求データを送信するとともに送信されてきたデータを受信する第1の送受信部と、

 上記データ送受信部によって受信されたデータを蓄える第1のデータ記憶部と、

- 10 上記第1のデータ記憶部から読み出されたデータを上記第1の記憶部に記憶されている上記第2の識別データに基づいて復号化処理を施す第1の信号処理部と、

- 上記第1の送受信部によって受信されたデータを上記第1のデータ記憶部に記憶させる動作を行うとともに上記第1のデータ記憶部から読み出されたデータの上記第1の信号処理部による復号化処理動作を制御する第1の制御部と、

 上記第1の送受信部から送信されてきた上記第1の識別データと上記配信要求データを受信するとともにデータの送信を行う第2の送受信部と、

- 20 複数のデータが記憶され、上記配信要求データに対応するデータを入力する第2のデータ記憶部と、

 上記送信されてきた第1の識別データに対応する第2の識別データが記憶されている第2の記憶部と、

- 上記第2のデータ記憶部から出力されたデータに上記第2の記憶部から読み出された第2の識別データに基づいて暗号化処理を施す第2の信号処理部と、

-----上記送信されてきた配信要求データと上記第1の識別データに基づいて-----
て上記第2の記憶部から上記第2の識別データの読み出し制御を行うとともに上記配信要求データに基づいて上記第2のデータ記憶部からデータの読み出し制御を行う第2の制御部とを備え、

- 5 上記第2の送受信部を介して送信されてきた上記第2の識別データに基づいて暗号化されたデータを上記第1の信号処理部によって復号するデータ配信装置。

2. 上記第2の制御部は、上記第1の送受信部から課金情報が上記第2の送受信部に送信され、上記送信されてきた課金情報に基づいて上記第10 2の記憶部からの上記第2の識別データの読み出しを制御する請求の範囲第1項記載のデータ配信装置。

3. 上記装置は、更に上記第2のデータ記憶部に書き込まれるデータに暗号化データに基づいて暗号化処理を施す暗号化処理手段を備え、上記暗号化処理手段によって暗号化されたデータは上記第2のデータ記憶部15 に書き込まれるとともに、上記配信要求データに基づいてデータを上記第2のデータ記憶部から読み出して上記第2の送受信部から上記第1の送受信部に送信する際に上記暗号化データを上記第2の信号処理部によって上記第2の識別データによって暗号化して上記第2のデータ記憶部から読み出されたデータとともに送信する請求の範囲第1項記載のデータ20 配信装置。

4. 上記第1の信号処理部は、上記第2の送受信部から送信されてきたデータと上記暗号化データを上記第1の記憶部に記憶されている上記第2の識別データによって復号するとともに、復号された暗号化データに基づいて復号されたデータに上記暗号化データによって施されている暗25 号の復号処理を行う請求の範囲第3項記載のデータ配信装置。

5. 上記第1の制御部は、上記暗号化データに基づいて課金処理を行う

請求の範囲第 3 項記載のデータ配信装置。

6. 上記暗号化データは動的に変化するデータ部を有し、上記第 1 の制御部は、上記第 1 のデータ記憶部に記憶されている上記第 2 の送受信部からデータとともに送信されてきた上記暗号化データのうち上記動的
- 5 に変化するデータ部を所定の時間毎に判別する請求の範囲第 4 項記載のデータ配信装置。

7. 上記第 1 の制御部は、上記動的に変化するデータ部の判別結果に基づいて上記第 1 のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第 6 項記載のデータ配信装置。

- 10 8. 上記第 1 の制御部は、上記動的に変化するデータ部の判別結果が上記暗号化データが正しくないときには少なくとも上記第 1 のデータ記憶部からのデータの読み出し動作を禁止する請求の範囲第 7 項記載のデータ配信装置。

9. 上記暗号化データは時間的に変化するデータ部を有し、上記第 1 の
- 15 制御部は、上記第 1 のデータ記憶部に記憶されている上記第 2 の送受信部からデータとともに送信されてきた上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲第 4 項記載のデータ配信装置。

10. 上記第 1 の制御部は、上記時間的に変化するデータ部の判別結果
- 20 に基づいて上記第 1 のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第 9 項記載のデータ配信装置。

11. 上記第 1 の制御部は、上記時間的に変化するデータ部の判別結果が所定時間を過ぎているときには少なくとも上記記憶部からのデータの読み出し動作を禁止する請求の範囲第 10 項記載のデータ配信装置。

- 25 12. 上記装置は、更に上記第 1 のデータ記憶部に記憶されているデータを移動するときに上記第 1 の信号処理部によって復号化されたデータ

-----に更にデータを移動する先の第1の識別データに基づいて暗号化処理を-----
施す更なる信号処理部を備えている請求の範囲第4項記載のデータ配信装置。

1 3. 上記第1の制御部は、上記第1のデータ記憶部に記憶されている
5 データの移動が終了した時点で上記第1のデータ記憶部に記憶されている
上記暗号化データを削除する請求の範囲第12項記載のデータ配信装置。

1 4. 機器固有の第1の識別データと上記第1の識別データと対応する
第2の識別データとが記憶されている第1の記憶部と、上記第1の記憶
10 部から読み出された上記第1の識別データとともにデータの配信要求デ
ータを送信するとともに送信されてきたデータを受信する第1のデータ
送受信部と、上記データ送受信部によって受信されたデータを蓄える第
1のデータ記憶部と、上記第1のデータ記憶部から読み出されたデータ
を上記第1の記憶部に記憶されている上記第2の識別データに基づいて
15 復号化処理を施す第1の信号処理部と、上記第1の送受信部によって受
信されたデータを上記第1のデータ記憶部に記憶させる動作を行うとと
もに上記第1のデータ記憶部から読み出されたデータの上記第1の信号
処理部による復号化処理動作を制御する第1の制御部とを有する少なく
ともひとつの端末機器部と、

20 上記端末機器部と伝送路を介して接続され、上記第1の送受信部から
送信されてきた上記第1の識別データと上記配信要求データを受信する
とともにデータの送信を行う第2の送受信部と、複数のデータが記憶さ
れ、上記配信要求データに対応するデータを出力する第2のデータ記憶
部と、上記送信されてきた第1の識別データに対応する第2の識別デー
25 タが記憶されている第2の記憶部と、上記第2のデータ記憶部から出力
されたデータに上記第2の記憶部から読み出された第2の識別データに

基づいて暗号化処理を施す第 2 の信号処理部と、上記送信されてきた配信要求データと上記第 1 の識別データに基づいて上記第 2 の記憶部から上記第 2 の識別データの読み出し制御を行うとともに上記配信要求データに基づいて上記第 2 のデータ記憶部からデータの読み出し制御を行う

5 第 2 の制御部とを有するサーバ装置部とを備え、

上記第 2 の送受信部を介して送信されてきた上記第 2 の識別データに基づいて暗号化されたデータを上記第 1 の信号処理部によって復号するデータ配信装置。

1 5. 上記第 2 の制御部は、上記第 1 の送受信部から課金情報が上記第

10 2 の送受信部に送信され、上記送信されてきた課金情報に基づいて上記第 2 の記憶部からの上記第 2 の識別データの読み出しを制御する請求の範囲第 1 4 項記載のデータ配信装置。

1 6. 上記装置は、更に上記第 2 のデータ記憶部に書き込まれるデータに暗号化データに基づいて暗号化処理を施す暗号化処理手段を備え、上

15 記暗号化処理手段によって暗号化されたデータは上記第 2 のデータ記憶部に書き込まれるとともに、上記配信要求データに基づいてデータを上記第 2 のデータ記憶部から読み出して上記第 2 の送受信部から上記第 1 の送受信部に送信する際に上記暗号化データを上記第 2 の信号処理部によって上記第 2 の識別データによって暗号化して上記第 2 のデータ記憶

20 部から読み出されたデータとともに送信する請求の範囲第 1 4 項記載のデータ配信装置。

1 7. 上記第 1 の信号処理部は、上記第 2 の送受信部から送信されてきたデータと上記暗号化データを上記第 1 の記憶部に記憶されている上記第 2 の識別データによって復号するとともに、復号された暗号化データ

25 に基づいて復号されたデータに上記暗号化データによって施されている暗号の復号処理を行う請求の範囲第 1 6 項記載のデータ配信装置。

- 1 8. 上記第 1 の制御部は、上記暗号化データに基づいて課金処理を行
う請求の範囲第 1 6 項記載のデータ配信装置。
- 1 9. 上記暗号化データは動的に変化するデータ部を有し、上記第 1 の
制御部は、上記第 1 のデータ記憶部に記憶されている上記第 2 の送受信
5 部からデータとともに送信されてきた上記暗号化データのうち上記動的
に変化するデータ部を所定の時間毎に判別する請求の範囲第 1 6 項記載の
データ配信装置。
- 2 0. 上記第 1 の制御部は、上記動的に変化するデータ部の判別結果に
基づいて上記第 1 のデータ記憶部に記憶されているデータの読み出し動
10 作を制御する請求の範囲第 1 9 項記載のデータ配信装置。
- 2 1. 上記第 1 の制御部は、上記動的に変化するデータ部の判別結果が
上記暗号化データが正しくないときには少なくとも上記第 1 のデータ記
憶部からのデータ読み出し動作を禁止する請求の範囲第 2 0 項記載のデ
ータ配信装置。
- 15 2 2. 上記暗号化データは時間的に変化するデータ部を有し、上記第 1
の制御部は、上記第 1 のデータ記憶部に記憶されている上記第 2 の送受
信部からデータとともに送信されてきた上記暗号化データのうち上記動
的に変化するデータ部を所定の時間毎に判別する請求の範囲第 1 6 項記載
のデータ配信装置。
- 20 2 3. 上記第 1 の制御部は、上記時間的に変化するデータ部の判別結果
に基づいて上記第 1 のデータ記憶部に記憶されているデータの読み出し
動作を制御する請求の範囲第 2 2 項記載のデータ配信装置。
- 2 4. 上記第 1 の制御装置は、上記時間的に変化するデータ部の判別結
果が所定時間を過ぎているときには少なくとも上記記憶部からのデータ
25 読み出し動作を禁止する請求の範囲第 2 3 項記載のデータ配信装置。
- 2 5. 上記装置は、更に上記第 1 のデータ記憶部に記憶されているデー

タを他の端末機器部に移動するときに上記第1の信号処理部によって復号化されたデータに更にデータを移動する先の上記他の端末機器部の第1の識別データに基づいて暗号化処理を施す更なる信号処理部を備えている請求の範囲第16項記載のデータ配信装置。

- 5 26. 上記第1の制御部は、上記第1のデータ記憶部に記憶されているデータの移動が終了した時点で上記第1のデータ記憶部に記憶されている上記暗号化データを削除する請求の範囲第25項記載のデータ配信装置。

27. 装置固有の第1の識別データと上記第1の識別データと対応する第2の識別データとが記憶されている記憶部と、

上記記憶部から読み出された上記第1の識別データとともにデータの配信要求データを送信するとともに上記第2の識別データによって暗号化されて送信されてきたデータを受信するデータ送受信部と、

- 15 上記データ送受信部によって受信された上記第2の識別データに基づいて暗号化されたデータを蓄えるデータ記憶部と、

上記データ記憶部から読み出されたデータを上記記憶部に記憶されている上記第2の識別データに基づいて復号処理を施す信号処理部と、

- 20 上記送受信部によって受信されたデータを上記データ記憶部に記憶させる動作を行うとともに上記データ記憶部から読み出されたデータの上記信号処理部による復号化処理動作を制御する制御部とを備えているデータ配信用の端末装置。

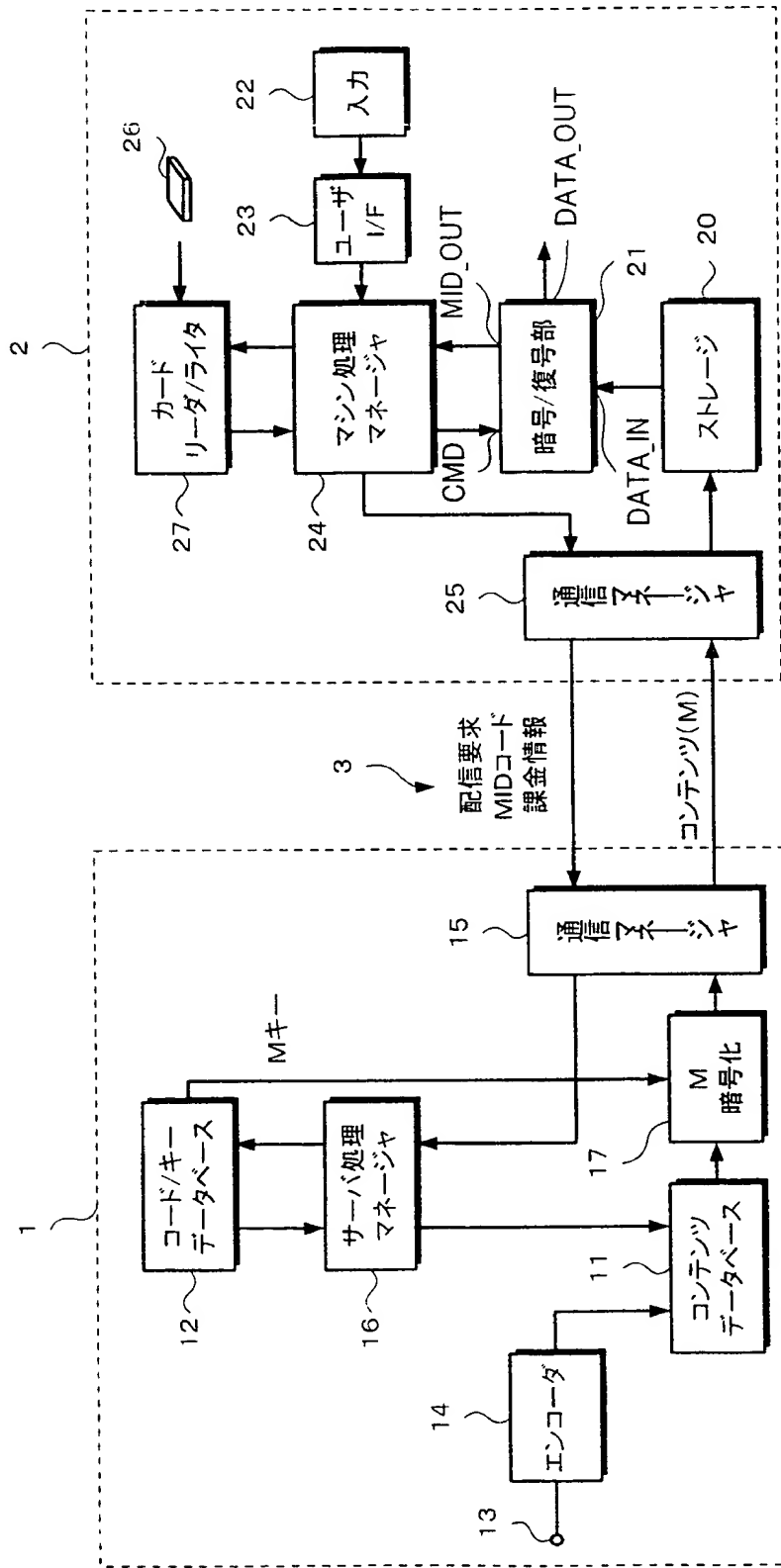
28. 上記データ記憶部には、上記データ送受信部によって受信されたデータと当該データに施されている暗号化に元となる暗号化データが記憶されており、上記信号処理部は、上記データ記憶部から読み出された
25 データを上記第1の記憶部に記憶されている上記第2の識別データによって復号するとともに、復号された暗号化データに基づいて復号された

- データに上記暗号化データによって施されている暗号の復号処理を行う請求の範囲第 27 項記載のデータ配信用の端末装置。
29. 上記第 1 の制御部は、上記暗号化データに基づいて課金処理を行う請求の範囲第 28 項記載のデータ配信用の端末装置。
- 5 30. 上記暗号化データは動的に変化するデータ部を有し、上記の制御部は、上記のデータ記憶部にデータとともに記憶されている上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲第 28 項記載のデータ配信用の端末装置。
31. 上記制御部は、上記動的に変化するデータ部の判別結果に基づいて上記データ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第 30 項記載のデータ配信用の端末装置。
- 10 32. 上記制御部は、上記動的に変化するデータ部の判別結果が上記暗号化データが正しくないときには少なくとも上記データ記憶部からのデータの読み出し動作を禁止する請求の範囲第 31 項記載のデータ配信用
- 15 の端末装置。
33. 上記暗号化データは時間的に変化するデータ部を有し、上記制御部は、上記データ記憶部にデータとともに記憶されている上記暗号化データのうち上記動的に変化するデータ部を所定の時間毎に判別する請求の範囲第 28 項記載のデータ配信用の端末装置。
- 20 34. 上記制御部は、上記時間的に変化するデータ部の判別結果に基づいて上記第 1 のデータ記憶部に記憶されているデータの読み出し動作を制御する請求の範囲第 30 項記載のデータ配信用の端末装置。
35. 上記制御部は、上記時間的に変化するデータ部の判別結果が所定時間を過ぎているときには少なくとも上記記憶部からのデータの読み出し動作を禁止する請求の範囲第 31 項記載のデータ配信用端末装置。
- 25 36. 上記装置は、更に上記データ記憶部に記憶されているデータを移

動するときに上記信号処理部によって復号化されたデータに更にデータを移動する先の第1の識別データに基づいて暗号化処理を施す更なる信号処理部を備えている請求の範囲第28項記載のデータ配信用端末装置。

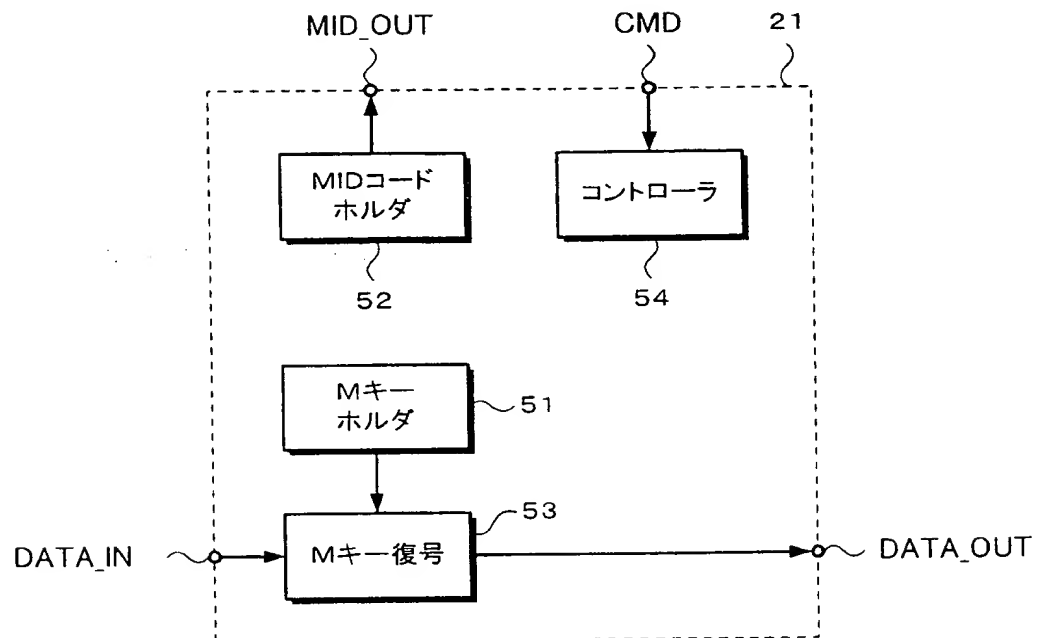
- 5 37. 上記制御部は、上記データ記憶部に記憶されているデータの移動が終了した時点で上記のデータ記憶部に記憶されている上記暗号化データを削除する請求の範囲第33項記載のデータ配信用端末装置。
-

第1図



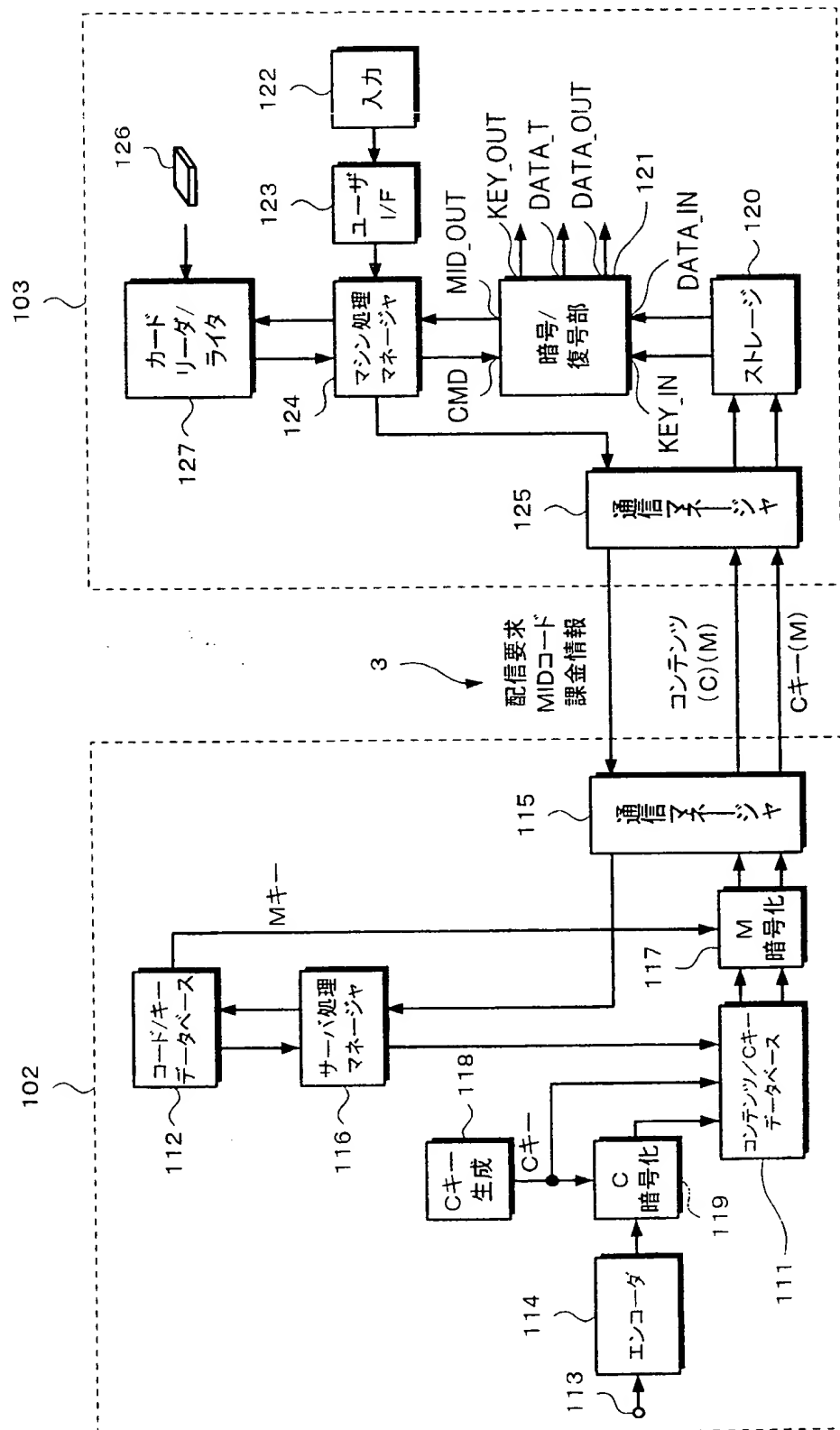
THIS PAGE BLANK (USPTO)

第2図



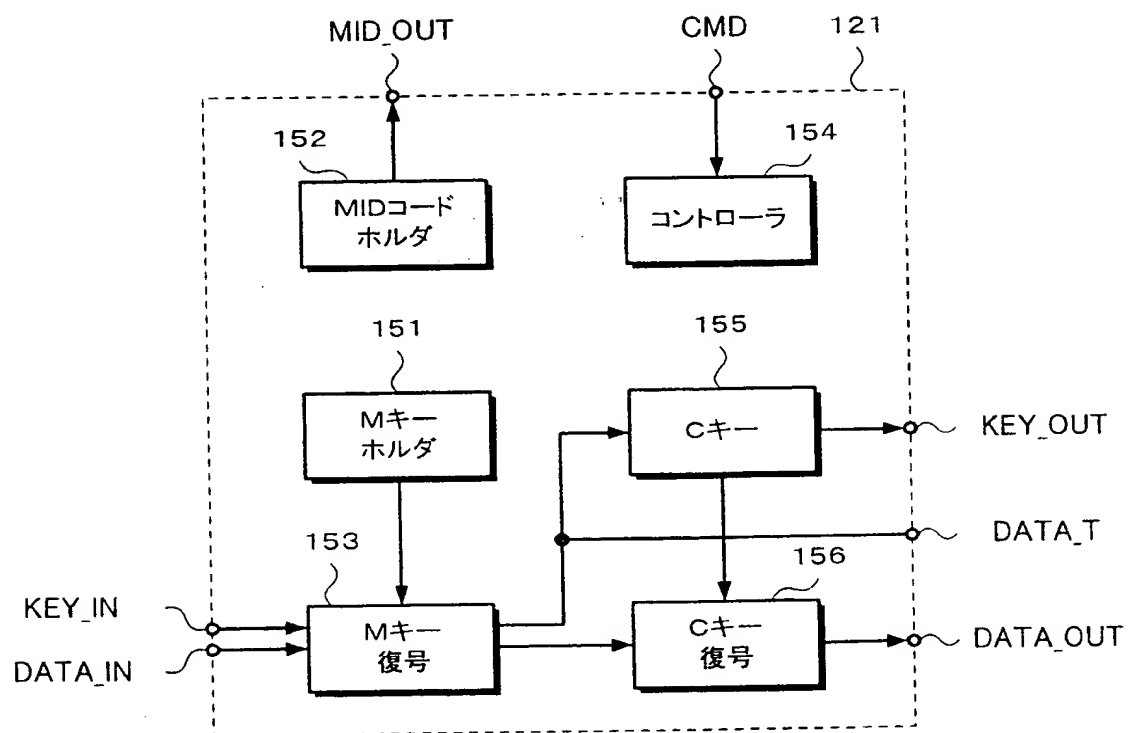
THIS PAGE BLANK (USPTO)

第3図



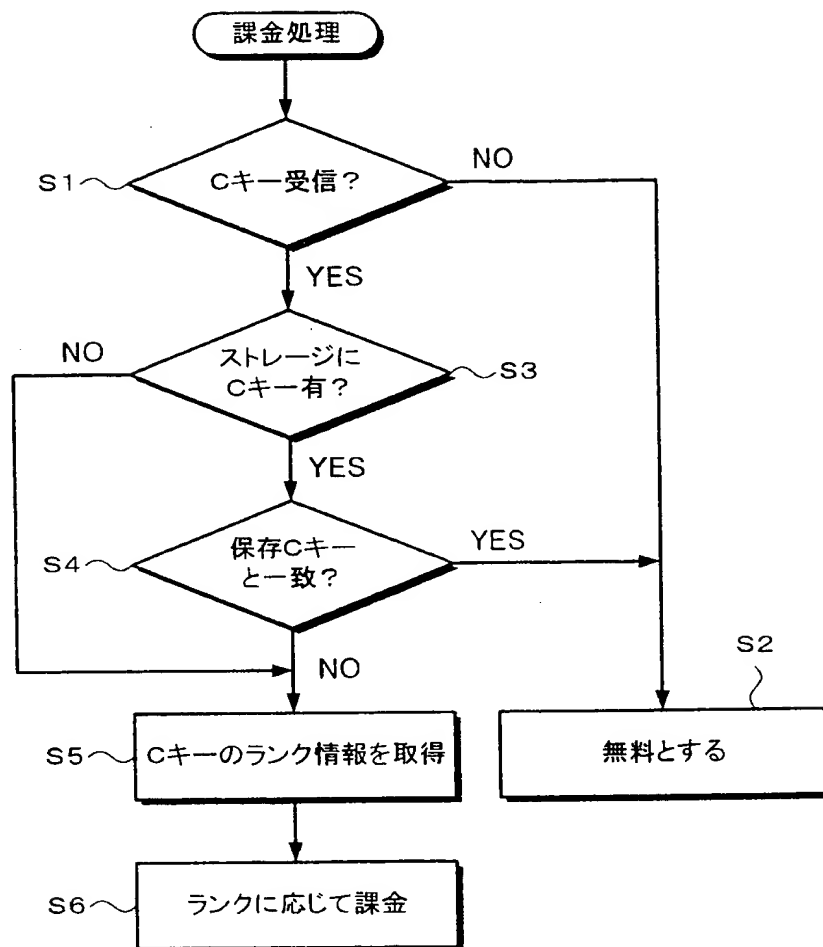
THIS PAGE BLANK (USPTO)

第4図



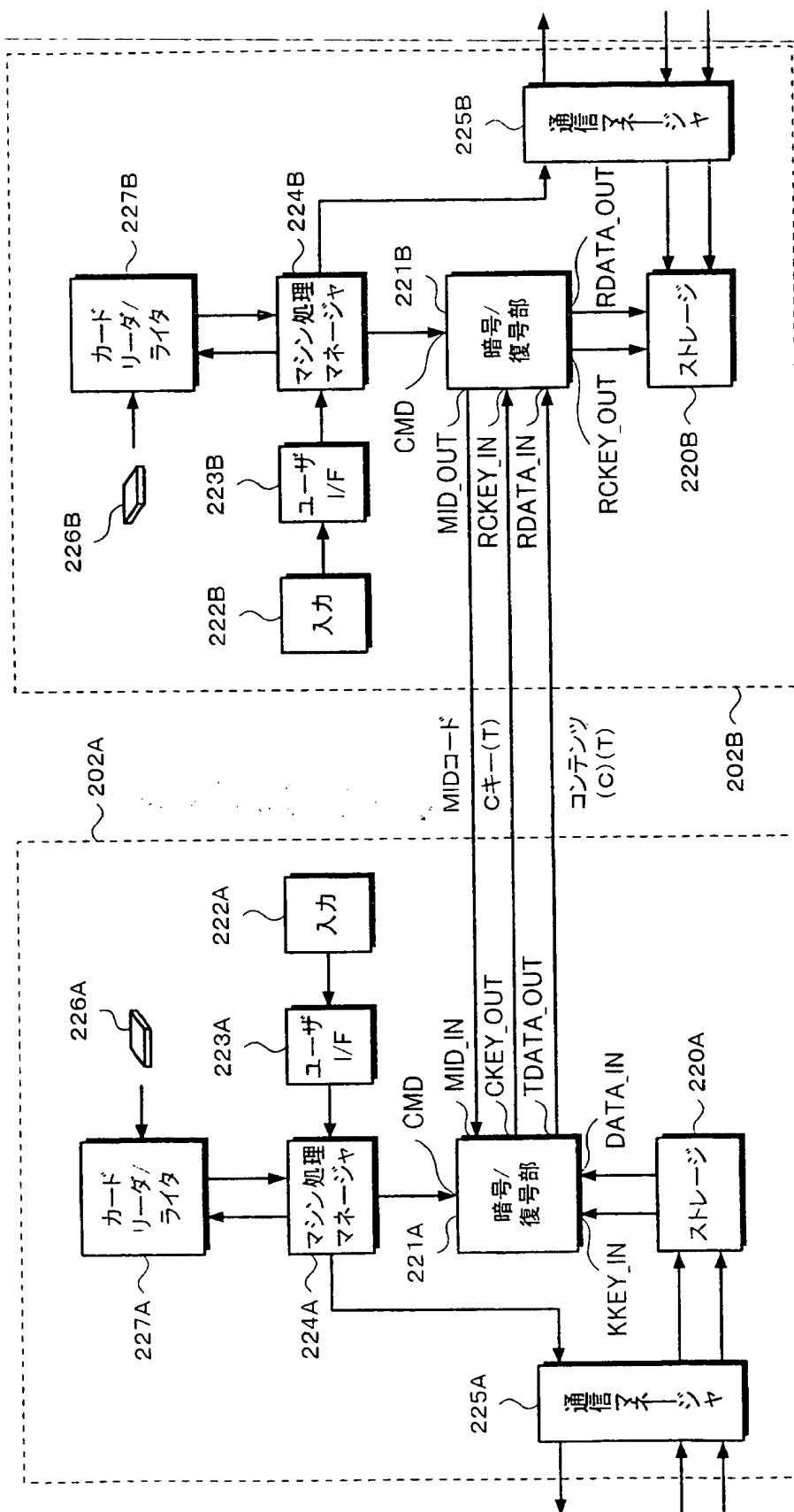
THIS PAGE BLANK (USPTO)

第5図



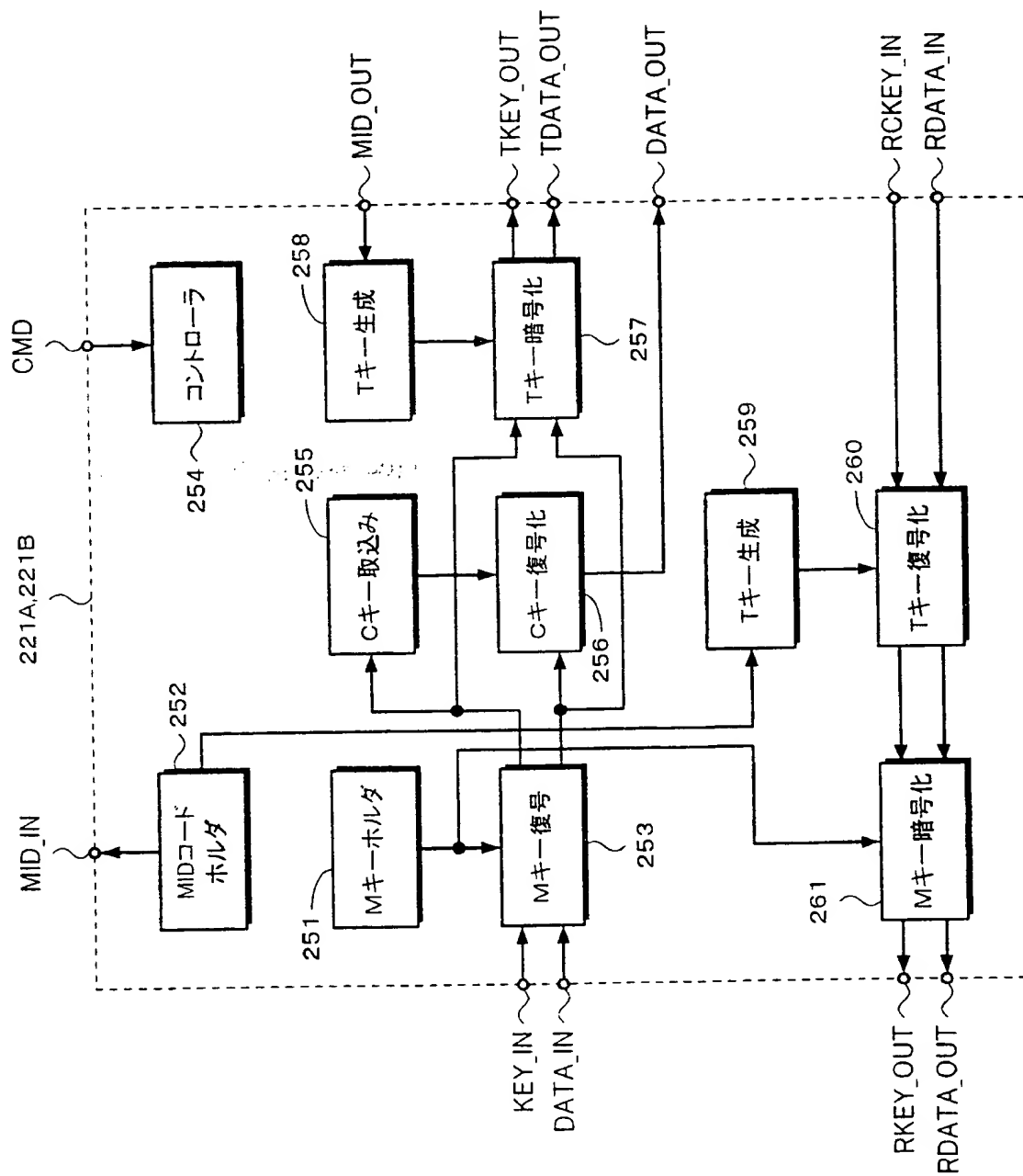
THIS PAGE BLANK (USPTO)

第6図



THIS PAGE BLANK (USPTO)

鋼

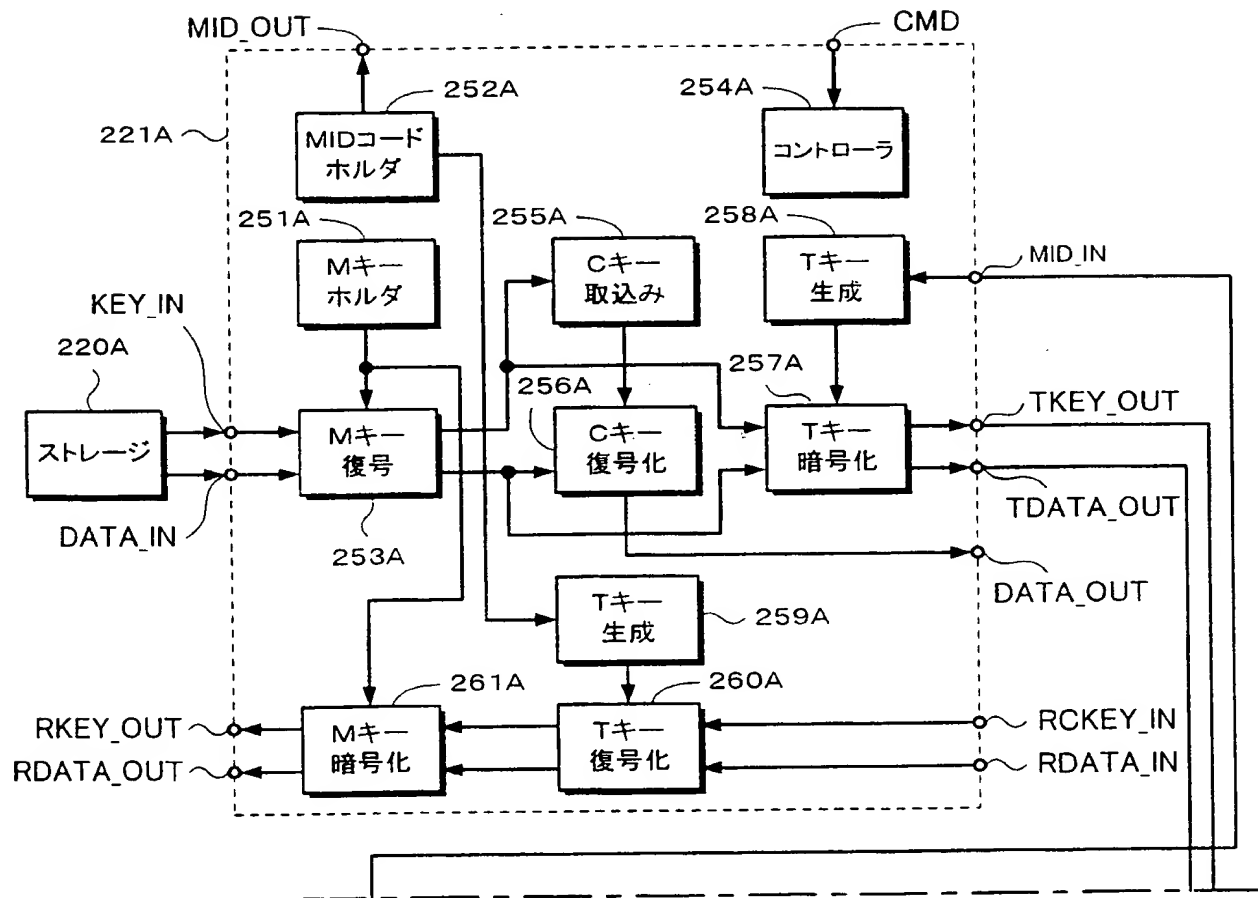


THIS PAGE BLANK (USPTO)

第8図

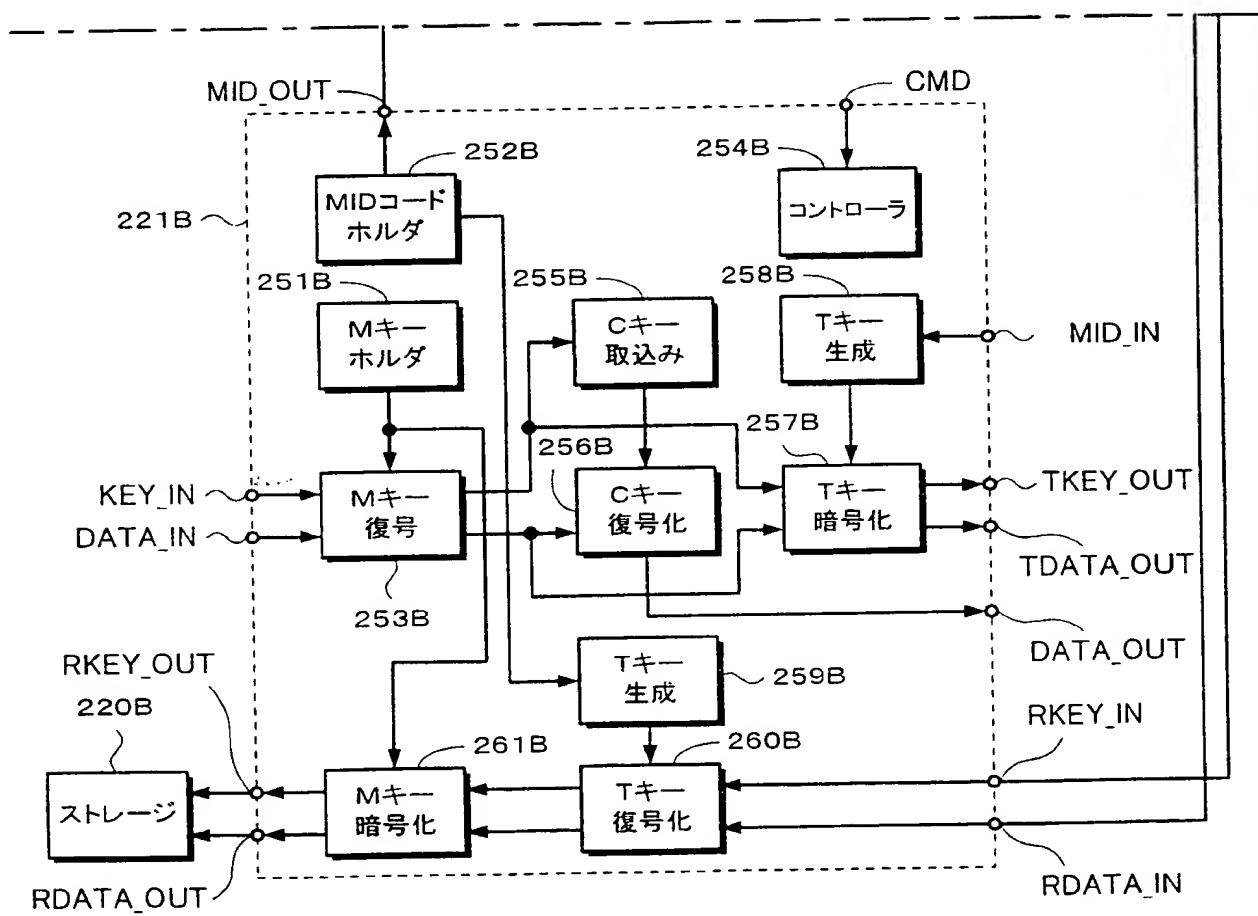
第8図A
第8図B

第8図A



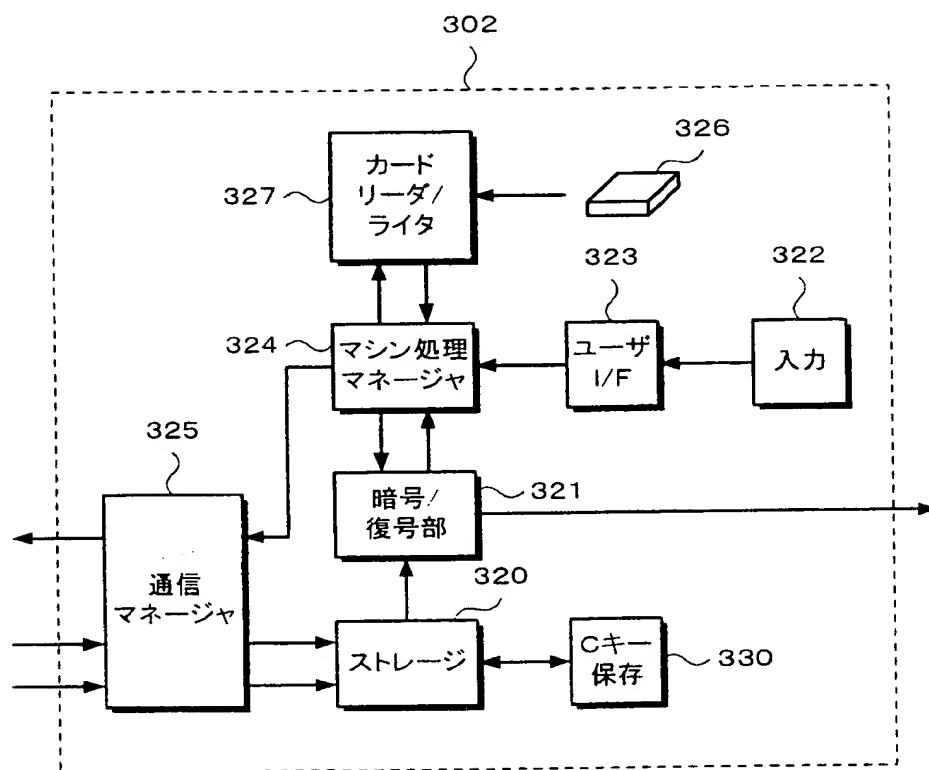
THIS PAGE BLANK (USPTO)

第8図B

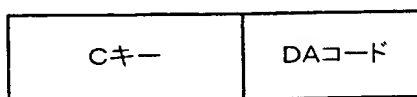


THIS PAGE BLANK (USPTO)

第 9 図

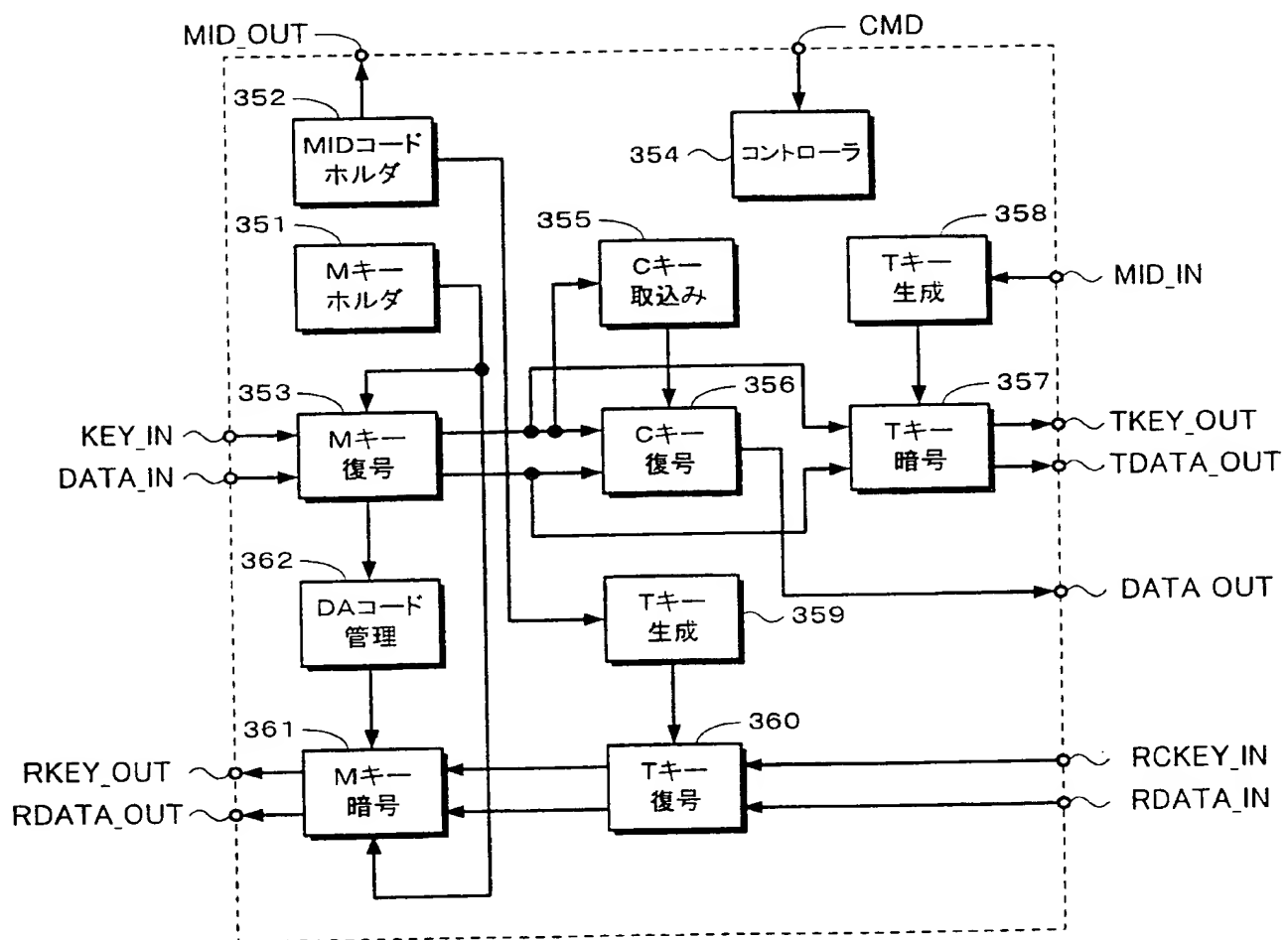


第 1 0 図



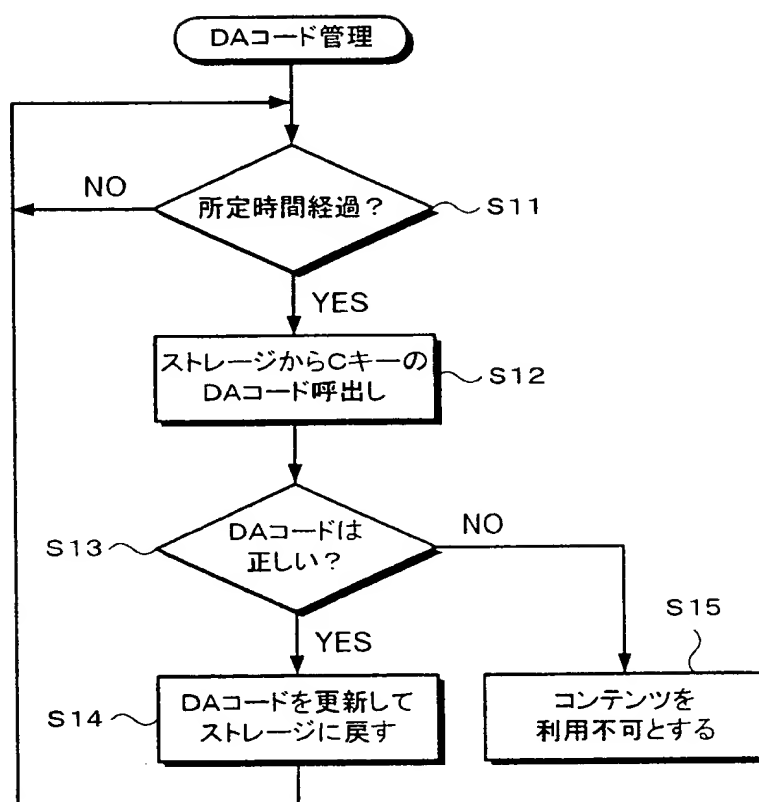
THIS PAGE BLANK (USPTO)

第 1 1 図



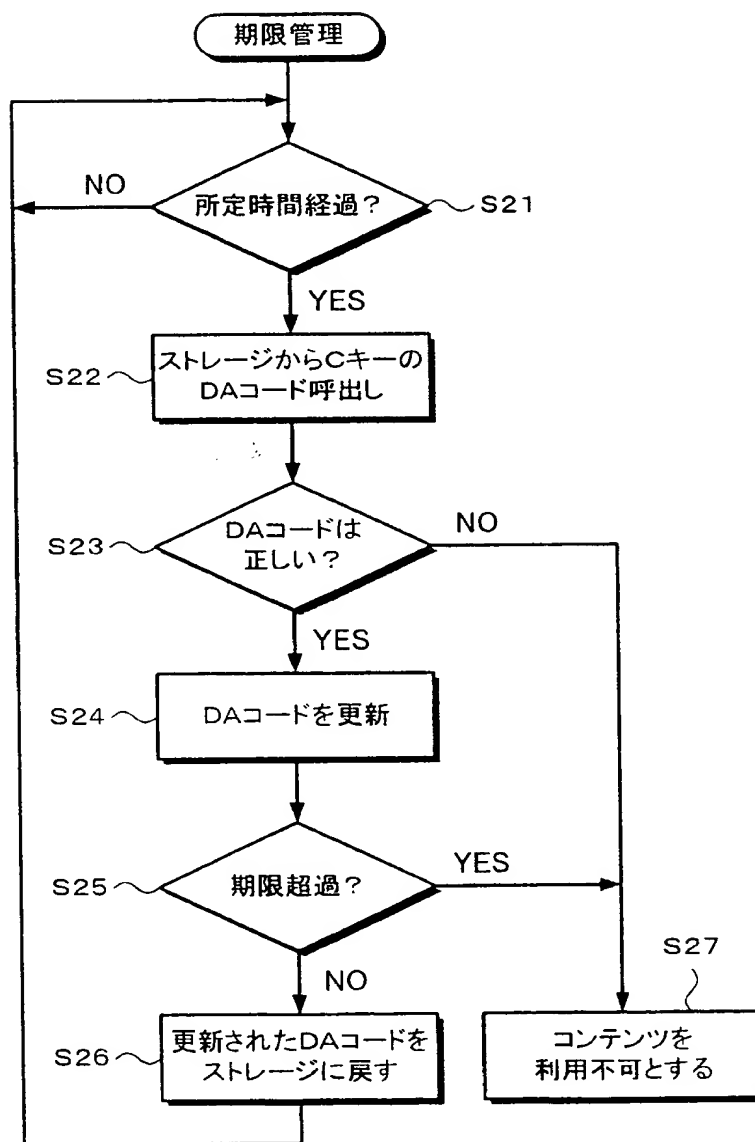
THIS PAGE BLANK (USPTO)

第 1 2 図



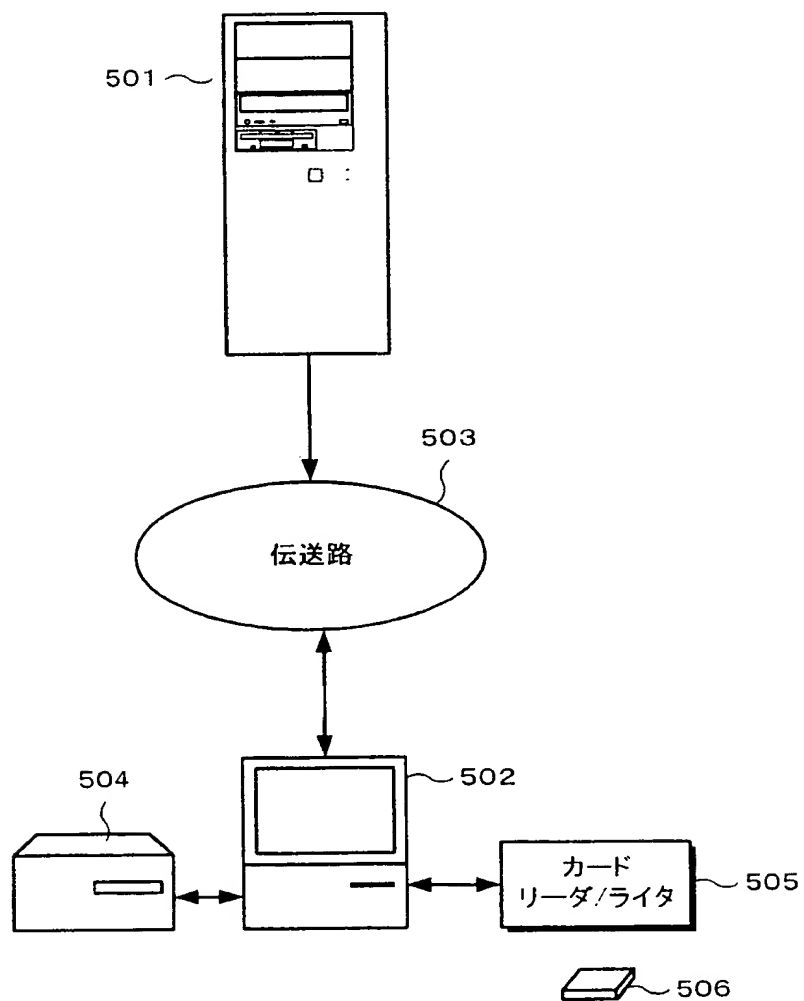
THIS PAGE BLANK (USPTO)

第 1 3 図



THIS PAGE BLANK (USPTO)

第 1 4 図



THIS PAGE BLANK (USPTO)

- 1、101・・・コンテンツサーバ
- 2、102、202A、202B、302・・・ユーザマシン
- 20、120、220A、220B、320・・・ストレージデバイス
- 21、121、221A、221B、321・・・暗号化／復号化処理チップ

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/02404

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁶ G06F17/60, G06F17/30, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁶ G06F17/60, G06F17/30, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 10-13808, A (Matsushita Electric Industrial Co., Ltd.), 16 January, 1998 (16. 01. 98) (Family: none)	1-37
A	JP, 9-269916, A (Hitachi, Ltd.), 14 October, 1997 (14. 10. 97) (Family: none)	1-37
A	JP, 8-8851, A (Toshiba Corp.), 12 January, 1996 (12. 01. 96) (Family: none)	1-37

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
27 July, 1999 (27. 07. 99)

Date of mailing of the international search report
10 August, 1999 (10. 08. 99)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁸ G 0 6 F 1 7 / 6 0, G 0 6 F 1 7 / 3 0, G 0 6 F 1 5 / 0 0

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁸ G 0 6 F 1 7 / 6 0, G 0 6 F 1 7 / 3 0, G 0 6 F 1 5 / 0 0

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996年
日本国公開実用新案公報	1971-1999年
日本国実用新案登録公報	1996-1999年
日本国登録実用新案公報	1994-1999年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 1 0 - 1 3 8 0 8, A (松下電器産業株式会社), 1 6. 1 月. 1 9 9 8 (1 6. 0 1. 9 8) (ファミリーなし)	1 - 3 7
A	J P, 9 - 2 6 9 9 1 6, A (株式会社日立製作所), 1 4. 1 0 月. 1 9 9 7 (1 4. 1 0. 9 7) (ファミリーなし)	1 - 3 7
A	J P, 8 - 8 8 5 1, A (株式会社東芝), 1 2. 1 月. 1 9 9 6 (1 2. 0 1. 9 6) (ファミリーなし)	1 - 3 7

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

2 7. 0 7. 9 9

国際調査報告の発送日

1 0.08.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

金子 幸一

印

5 L

8 7 2 4

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 6 0

THIS PAGE BLANK (USPTO)